A BAYESIAN RELIABILITY STUDY ON MOTORIZED VALVES FOR THE EMERGENCY CORE COOLING, HEAT TRANSPORT ISOLATION AND SHUTDOWN COOLING SYSTEMS AT GENTILLY-2 NUCLEAR GENERATING STATION

JAMES E. SMITH, DONALD F. RENNICK, ALINA NAINER

Cantech International Ltd

MICHEL DEMERS, RAYNALD VAILLANCOURT

Hydro-Québec, Gentilly-2 NGS

ABSTRACT

The objective of this study is to examine operational data on 32 motorized valves in the emergency core cooling, shutdown cooling and heat transport isolation systems and determine if the evidence would support a reduction in testing frequency of these valves. The methodology used is to examine the data which has accumulated on motorized valve failures since Gentilly-2 first entered service, compare these data with similar data from other sources, and determine whether the evidence indicate that demand-based, wearout type failure mechanisms play a significant role in the recorded failures. The statistical data are then updated, using a Bayesian updating procedure, to obtain revised time based failure rates and demand based probabilities of failure on demand for the motorized valves. The revised failure rates and probabilities are then applied to the fault tree models for the systems of interest to determine what effect there would be, with the current test intervals and with extended test intervals, on the probability of failure of the systems.

1. INTRODUCTION

Hydro-Québec has experienced some problems with motorized valves in the past. Such problems include:

(a) Leakage from the valves' packings.
(b) Damage and wear to the valve seats.
(c) Failures of the valve actuators.

There is some concern that these problems may be related to the frequency of testing, ie. that the failures are demand based, rather than time based, as has always been assumed in the past. Thus there is a need to determine whether certain failure modes and mechanisms are demand based and whether a reduction in the number of demands can improve the overall reliability of the valves.

Each of the above types of valve failure can cause other problems, which make it desirable to minimize the frequency of such failures. Leakage from the valves' packing can result in increased tritium in containment, causing increased radiation exposure for maintenance crews when work has to be done in containment. Damage and wear to the valve seats can cause particles of radioactive cobalt to be loose in the heat transport and auxiliary systems, again adding to the risk of exposure. Failures of the valves' actuators may cause the valves to fail to function at a critical time. These failure modes and mechanisms are examined subsequently in more detail in this paper.

This study examines the data available for 32 motorized valves to determine if the failure mechanisms associated with these failure modes are demand based or time based, and whether reduction of testing frequencies can be justified on that basis.

2. VALVE CLASSIFICATION

This study examines a relatively small number of valves at Gentilly-2. Thus there is a small statistical database. In order to provide a statistically significant database for numerical evaluation of failure rates, it is necessary to include motorized valve failure data from other sources. These include:

(a) European Industry Reliability Data Bank
(b) Ontario Hydro Reliability Data
(c) Pt. Lepreau NGS Component Reliability Statistics.

In order to ensure a reasonable degree of compatibility of data it is necessary to classify the valves at Gentilly-2 by size, type and function, into generic classes that fit with the data from these other sources.

2.1. Classification by Size

The European data includes valves from a very wide size range in a single classification, therefore it is used for all valve sizes from Gentilly-2. However, both Ontario Hydro and Pt. Lepreau do classify their data by specific size ranges. Thus the same size ranges is used for the Gentilly-2 valves. These size ranges are:

(a) Less than 2"
(b) 2" or greater, but less than 6"
(c) 6" or greater, but less than 12"
(d) 12" or greater but less than 24"

2.2. Classification by Type

Of the valves under consideration at Gentilly-2, only two types have been identified, namely gate valves and globe valves. Similar classifications are available for Ontario Hydro and Pt. Lepreau data. In the European data, valve types are identified as "paraslide", which is assumed to be the same as "gate", "swing" which is assumed to be the same as "butterfly", and a third data set includes all types of motorized isolation valves.

2.3. Classification by Function

Without exception, the valves under consideration at Gentilly-2 are isolation valves. However, with the reactor operating normally, some are normally closed and would be expected to open in an accident or shutdown scenario, while others are normally closed and would be expected to open. Those valves that are normally open with the reactor at power are designated "NO". Those valves that are normally closed with the reactor at power are designated "NC".

2.4. Classification Results

There are 6 broad classes that can be examined, namely:

1. Globe valves, ≥ 2", < 6", normally closed when the reactor is at power.
2. Globe valves, ≥ 2", < 6", normally open when the reactor is at power.
3. Gate valves, ≥ 6", < 12", normally open when the reactor is at power.
4. Gate valves, ≥ 6", < 12", normally closed when the reactor is at power.
5. Gate valves, ≥ 12", < 24", normally closed when the reactor is at power.
6. Gate valves, ≥ 12", < 24", normally open when the reactor is at power.

3. MODES AND MECHANISMS OF FAILURE

Functional failure modes are the failure modes depicted in the fault tree models for the systems. For the types of motorized valve under consideration, they are:

(a) Opens or closes spuriously
(b) Fails to open or close when required
(c) External leakage
(d) Internal leakage, ie. the valve is still passing fluid when it is supposed to be fully closed.

For a motorized isolating valve, mode (a) is usually associated with control failure mechanisms that lead to the actuator being energized when it is not required to be energized. On rare occasions the valve may change position spuriously due to a failure of the valve's internals, eg. the stem of a gate valve fractures and the gate falls into the closed position under gravity. However, such failure mechanisms occur extremely rarely, and for most practical cases can be discounted.

Mode (b) may be caused by a variety of failure mechanisms. The valve controls may fail to energize the actuator when required, or may try to drive it in the wrong direction. If the valve is not exercised regularly, the mechanism may jam in place due to corrosion or failure of lubrication with time, and the actuator may not be able to apply sufficient force to free it. Similarly, if the fluid is dirty, foreign matter may jam the mechanism. The actuator itself may fail, or may become contaminated with foreign matter so that it ceases to work.

Mode (c) is most often associated with leakage, in small quantities, from seals or packing. Such leakage usually occurs when the seals and/or packing are worn, distorted or damaged. Wear and damage may be caused by the valve being exercised too much. Distortion of seals and packing may be caused by improper installation, and this may also lead to damage. Leakage may also occur due to cracking or fracture of the valve body or bonnet. However, like stem fractures, such failure mechanisms are very rare, and for most practical cases can be discounted.

Mode (d) is most likely to be caused by either control failures or by wear or damage to the valve seat. The control failures are likely to be failures of limit switches or torque switches, which limit the travel of the valve such that it stops prematurely. Wear or damage to the valve seat can be caused by exercising the valve too much or by foreign matter in the fluid.

Table 1 shows the failure modes and mechanisms of interest for the valve classes. Examining table 1 shows that the differences among the failure modes and mechanisms are dictated by the normal operating position of the valve.

This discussion centres on the failure modes and mechanisms of the valves themselves that are modelled in reliability and probabilistic safety analyses. Control failures are modelled in their own right, in the systems' fault trees therefore their data do not figure in the determination of the valves' failure rates. However, the control failures should not be ignored in the overall discussion on test frequencies. The tests are the only way to determine if the controls are working or have failed too. For the purposes of discussion, control failures will be considered as time based.

A failure of a valve's internal mechanism that leads to a spurious opening or closing of the valve, eg. a stem fracture is likely to be a randomly occurring, low probability event. Therefore it is considered reasonable to treat such failures as randomly occurring in time.

Jamming of a valve due to corrosion of the internals is only likely to occur in valves that are subject to corrosive fluids and are not regularly tested, ie they are left in one position long enough to jam. For most of the valves in this study this would be unlikely to occur. However the failure mechanism is more associated with time than with demands.

Jamming of the valve due to foreign matter is, again, a very unlikely occurrence on the valves in this study, because the systems are usually kept clean. Particles of foreign matter large enough to jam the mechanisms would be unlikely to occur. However, such foreign matter as is generated by the valves themselves is more a function of demands than of time, because the moving parts and the valve seats are not subject to wear and friction unless the valves are called upon to change position. Thus this failure mechanism is regarded as a demand based mechanism.

Actuator internal failure is regarded as a demand based failure mechanism, because the actuator is not under stress unless the valve is called upon to change position. When the valve is called upon to change position, the actuator is subjected to both mechanical and electrical stress. Mechanical stress in overcoming the friction in the valve mechanism. Electrical stress in subjection to high motor starting current.

Actuator contaminated is regarded as a time based failure. The contamination could be either from external sources or could be from deterioration of the lubricant or grease within the actuator. Contamination from external sources would take time to build up to a point where it causes a problem. Deterioration of grease or oil from exposure to heat or radiation also takes time to reach a point where it causes a problem, independent of the demands placed on the valve.

External leakage through the seals or packing is considered to be a demand based failure mechanism. The leakage would be caused by wear to the seals or packing which occurs when the valve is required to change position.

Cracking of the valve body is regarded as a very low probability time based event. The stressing of the valve body due to demands is not likely to make a great deal of difference to the stressing from maintaining a pressure boundary. Thus cracking and rupture of a valve body is likely to occur randomly in time.

Damage or wear to the valve seat would be exclusively demand based for normally closed valves, because the only source of friction and wear at the valve seat would be when the valve changed position. For normally open valves there is an element of time dependence because of erosion by the fluid flow over the valve seat. However, since the fluid in the systems under consideration is clean water, the erosive element is probably very small, and the friction and wear is dominated by the demands placed upon the valves to change position.

4. OBSERVED FAILURES OF MOTORIZED VALVES

4.1. Gentilly-2 Data

The observed failures recorded in the quarterly technical reports, for the valves in the ECC, SDC and HTS isolation systems are reviewed against the criteria discussed in section 3. The results have been sorted by valve class and by whether the failure observed should be regarded as time based or demand based.

Given the time period over which the observations were made, estimates are then made for the total operational time for the valves, and the number of demands placed on the valves. For the total operational time, it is estimated that the station has been in service for 4566 days over the period of observation. This means that each valve has 4566 x 24 = 109 584 hours in service. Note that, for convenience, the initial reliability calculations for time based failures are performed to a base of hours in service. When final estimates for failure rates are made, the failure rates are converted to the more usual failures per 10^3 years. Similarly, since the observations are made over a period of 150 months, most of the valves were subjected to 150 demands each.

Table 2 summarizes the observed failure data together with point estimate calculations for time based failure rate and demand based probability of failure. Note that the control failures are ignored in the calculations of the reliability figures for the valves of Gentilly-2.

4.2. Other Sources of Data

As a precursor to the actual evaluation of the reliability figures by Bayesian methods, the data from Europe, Pt. Lepreau and Ontario Hydro were also examined.

Note that since it is not possible to make a firm determination of the demand based and time based failures for the Pt. Lepreau and Ontario Hydro data, it was decided to combine the Gentilly-2 and European data to obtain ratios that could be applied to the Pt. Lepreau and Ontario Hydro data to obtain estimates for numbers of time based and demand based failures. This assumes that both the Pt Lepreau and Ontario Hydro valves exhibit the same proportions of demand based and time based failures. Since the European and Gentilly-2 data showed fairly close agreement, this is considered a reasonable assumption.

The actual ratios are:

Demand based failures: (28 + 33) ÷ 77 = 0.792

Time based failures: (8 + 8) ÷ 77 = 0.208

For the Pt Lepreau data, no Globe valves were included. The valves could not be identified as NO or NC, and the failures of the limitorque switches in the actuators are recorded separately. The overall rates and probabilities of failure do not differ significantly from those observed at Gentilly-2.

The Ontario Hydro data is from Report No. 86296, published in 1986 and does not include any data from Darlington, or from the other Ontario Hydro stations since 1986. Such additional data is available, but it is not in an easily digested form at present. The effort required to obtain full, up-to-date Ontario Hydro data on all these motorized valves would be prohibitive for the scope of this study. As with Pt Lepreau, there are no data for globe valves. Since the notes in the report indicate that the observed failures include actuator failures, it is assumed that failures of the limitorque switches are also included. This assumption is also considered reasonable, because, in the section of 86296 devoted to instrumentation and control components, there are no records for limitorque switches. The overall rates and probabilities of failure do not differ significantly from those observed at Gentilly-2.

As we can see in table 2 concerning the overall Canadian data. the fact that the rates and probabilities of failures do not differ significantly from utility to utility, nor from the overall average is considered an indication that the assumptions are reasonable and will not lead to major inconsistencies.

5. EVALUATION OF RATES AND PROBABILITIES OF FAILURE

5.1. Time Based Failure Rates

The evaluation of the time based failure rates uses a two stage Bayesian updating process. For the prior data for the first stage, the European data is used. It is assumed that the prior distribution is the chi-squared distribution. The chi-squared distribution is used because the time based failures are expected to occur randomly in time, with times to failure distributed exponentially. Thus the failure rates or mean times between failure (MTBF) are distributes as chi-squared.

A Poisson likelihood function is used because we are dealing with relatively rare events with the failures of these valves. The failure rates are small so the Poisson function is the best model for this application.

The update data for the first stage of updating is the overall Canadian data.

The posterior distribution for the first stage becomes the prior distribution for the second stage. The updating process is repeated, using the Gentilly-2 specific data for the update data. The posterior distribution form the second stage of updating will be regarded as the new Gentilly-2 specific data and will be used to derive point estimates of failure rates for use in the fault tree models.

Note that, for convenience of calculation, MTBF is used throughout the Bayesian updating rather than failure rate.

5.2. Demand Based Probabilities of Failure

The Bayesian updating process for the demand based failures needs a slightly different approach. The original intention was to follow the same procedure as for the time based failures with the European data as the prior distribution, the overall Canadian data as the first update and the Gentilly-2 specific data as the second update. However, on the first attempt to follow this procedure, it was apparent that the likelihood figures were so small that it was not possible that the European data and the Canadian data were part of the same population as far as demand based failures were concerned. Therefore, only a single stage procedure is used, with the overall Canadian data as the prior distribution and the Gentilly-2 data as the only update.

There is another difference in the application in the choice of the prior distribution. Examination of the demand based failures for Gentilly-2 indicate that there is an element of wearout types of failure mechanism in those failures. Thus the times between failures would not be expected to be distributed exponentially. Also the

3. The actual valve designs may be sufficiently different that the two sets of data may not belong to the same overall population.

4. There may be preventive maintenance programs in place in Europe that preclude the occurrence of some failure modes observed in the Canadian data.

However, these are only speculative. One thing is remarkable though, that the proportion of time based to demand based failures was very similar between the European data and the observations at Gentilly-2.

7.3. Effects of Using Demand Based Probabilities of Failure on Valve Unavailabilities

Given a monthly test interval, as is the case for most of the valves in the study, and using the figures recommended in section 5.3, the probability of failure of a valve at each demand would be:

$$5.2 \times 10^{-3} + 5.0 \times 10^{-4} = 5.7 \times 10^{-3}$$

Comparing this with, say, a monthly test interval on a gate valve, size c, using Ontario Hydro data for time based failures alone, gives a probability of failure of:

$$1.295 \times 10^{-1} \times 0.0833 \times 0.5 = 5.4 \times 10^{-3}$$

There is little to choose between these figures. However, if we consider a test interval of three months, the corresponding figures would be:

$$5.2 \times 10^{-3} + 1.5 \times 10^{-3} = 6.7 \times 10^{-3} \quad \text{(demand based plus time based)}$$

$$1.295 \times 10^{-1} \times 0.25 \times 0.5 = 1.62 \times 10^{-2} \quad \text{(time based only)}$$

Thus there is a small increase in the overall probability of failure (17.5%) where valves are treated as having demand based and time based failure mechanisms, while there is a large increase in probability of failure where valves are treated as having time based probabilities of failure only (300%).

The full effects are evaluated in the fault tree models, because the valve tests also check on the availability of the control circuits, and the contribution from the controls needs to be factored into calculations. However, on the basis of the valve statistics alone there is a good case for reducing the frequency of testing, without significantly increasing the predicted unavailability of the valves, and hence the systems.

7.4. Fault Tree Analysis Results.
7.4.1. Shutdown Cooling System.

The original version of the fault tree logic showed only one failure event for each valve, and its probability of occurrence was calculated using only time based reliability data. The revised fault tree logic shows both time based and demand based failure modes for each valve. The failure rates and probabilities of failure on demand used in the evaluation of the fault tree are those derived in this study.

For operating in shutdown cooling pump mode, the fault tree top event probability does increase with increasing length of test interval. For the heat transport pump mode, increasing the length of the test interval makes no significant difference. This is because the motorized valves are effectively redundant in the heat transport pump mode, and so make no significant contribution to the top event probability.

The limiting case is the shutdown cooling pump mode. Here the motorized valves do make a significant contribution to the top event probability. However, increasing the test interval to 3 months results in only a 12% increase in the fault tree top event probability. Therefore, it is considered reasonable to recommend that the test interval for the motorized valves in the shutdown cooling system should be increased to 3 months. The increase in the predicted unreliability for the system is small and the benefits in reducing the incidence of demand based failures of the motorized valves could outweigh that increase in the future.

7.4.2. Emergency Core Cooling

The files for the High Pressure ECC, Medium Pressure ECC and Low Pressure ECC Initiation were modified in the same manner as described in section 7.4.1 for the shutdown cooling.

Figure 2 show the results of evaluating the fault trees, with test intervals for the motorized valves ranging from the current 1 month to 6 months. The results are similar to those for the shutdown cooling system. The top event probability does increase, in each case, with increasing length of test interval. However, the increase at 3 months is sufficiently small that the penalty in predicted system unavailability may well be offset by the reduced incidence of valve failures due to demand based failure mechanisms.

8. CONCLUSIONS

1. Based on the statistical evidence from this study, there is a good case for reducing the frequency of testing of motorized valves to reduce the failures which occur due to demand based failure mechanisms.

2. The case may be further supported by engineering arguments that reducing the testing frequency will also reduce the incidence of observed failures due to wearout type, demand based failure mechanisms, which would further reduce the statistical probability of failure. However, there are still time based, random failure mechanisms which need to be checked, therefore there is a limit to the reduction in frequency that can be allowed.

3. The results of revised fault tree analyses are probably conservative, because the revised reliability numbers used in the analyses were for all valve types and sizes and all failure modes.

9. REFERENCES

(1) G. APOSTOLAKIS, S. KAPLAN, B.J. GARRICK, R.J. DUPHILY, "Data Specialization for Plant Specific Risk Studies", Nuclear Engineering and Design, 1980.
(2) KAPLAN AND GARRICK, "On the Use of Bayesian Reasoning in Safety and Reliability Decisions - Three Examples", Nuclear Technology, 1979.
(3) FERGUSON, T.L., "Implementation Challenges of a Motor Operated Valve Program", Proceedings of the Third CANDU Maintenance Conference, pages 87-91, 1995 November.
(4) NUMET ENGINEERING/ SPECTRUM ENGINEERING CORP. LTD., "Aging and Malfunction of Valves in CANDU Special Safety Systems, AECB Project 2.115.1", AECB-INFO-0303, 1989 March.
(5) FOSTER MILLER INC., "Valve Motor Operator Improvements", EPRI Report NP-5696, 1989 July.
(6) HYDRO-QUÉBEC, "Quarterly Technical Report for Gentilly-2 Nuclear Generating Station", 1983 to 1995.
(7) H. PROCACCIA, P. AUFORT, S. P. ARSENIS, "European Industry Reliability Data Bank", Volume 2, Second Edition, European Safety Reliability & Data Association (ESReDA), 1995.
(8) ONTARIO HYDRO, "Component Reliability Data for CANDU Nuclear Stations", Report No. 86296, 1986.
(9) POINT LEPREAU GENERATING STATION, "Observed Component Reliability Data", Report No. IR-01530-01, 1995 February.

TABLE 1. FAILURE MODES AND MECHANISMS

VALVE CLASS	FAILURE MODE	FAILURE MECHANISM
Globe, b, NC	Opens spuriously	Controls spuriously energize actuator Internal failure
	Fails to open when required	Controls fail to energize actuator Valve mechanism jammed - corosion etc. Valve mechanism jammed - foreign matter Actuator internal failure Actuator contaminated
	Fails to reclose after test	Controls fail to energize actuator Valve mechanism jammed - foreign matter Actuator internal failure Actuator contaminated
	External leakage	Seals/Packing worn, distorted or damaged Valve body cracked
	Internal leakage	Control failure - not fully closed Valve seat worn or damaged.
Globe, b, NO	Closes spuriously	Controls spuriously energize actuator Internal failure
	Fails to close when required	Controls fail to energize actuator Valve mechanism jammed - corosion etc. Valve mechanism jammed - foreign matter Actuator internal failure Actuator contaminated
	Fails to reopen after test	Controls fail to energize actuator Valve mechanism jammed - foreign matter Actuator internal failure Actuator contaminated
	External leakage	Seals/Packing worn, distorted or damaged Valve body cracked
	Internal leakage	Control failure - not fully closed Valve seat worn or damaged.
Gate, c, NO	As Globe, b, NO	As Globe, b, NO
Gate, c, NC	As Globe, b, NC	As Globe, b, NC
Gate, d, NO	As Globe, b, NO	As Globe, b, NO
Gate, d, NC	As Globe, b, NC	As Globe, b, NC

TABLE 2. OBSERVED FAILURE DATA SUMMARY - CANADIAN DATA

All Valve Classes - All Failure Modes

Source	Observed Failures	Time Based	Demand Based	Operational Time (hrs)	No. of Demands	Time based Failure rate (f/1E6 hr)	Prob.of failure per demand
Gentilly-2 *	36	8	28	5 040 864	6600	1,59	0,0042
Pt. Lepreau	58	12	46	6 216 096	8850	1,93	0,0052
Ontario Hydro	216	44	172	31 325 760	34 680	1,40	0,005
Total	310	64	246	42 582 720	50 130	1,50	0,0049

* Observed failures exclude control failures

TABLE 3. SUMMARY OF EVALUATION OF FAILURE RATES

Data Type	Time Based		Demand Based	
	Mean Estimate Failure Rate (Failures/yr)	Median Estimate Failure Rate (Failures/yr)	Mean Estimate Probability of Failure	Median Estimate Probability of Failure
European (prior)	4,320E-03	4,678E-03	n/a	n/a
Canadian Overall	1,164E-02	1,123E-02	4,912E-03	5.224E-03
G-2 All Valves, All Modes	1,222E-02	1,157E-02	4,433E-03	4,517E-03
G-2 Globe, b, NC	1,207E-02	1,149E-02	4,703E-03	4,985E-03
G-2 Globe, b, NO	1,138E-02	1,104E-02	3,247E-03	3,324E-03
G-2 Gate, c, NC	1,179E-02	1,137E-02	5,053E-03	5,191E-03
G-2 Gate, c, NO	1,229E-02	1,157E-02	9.879E-03	1,128E-02
G-2 Gate, d, NC	1,146E-02	1,110E-02	3,247E-03	3,324E-03
G-2 Gate, d, NO	1,155E-02	1,116E-02	3.706E-03	3,831E-03

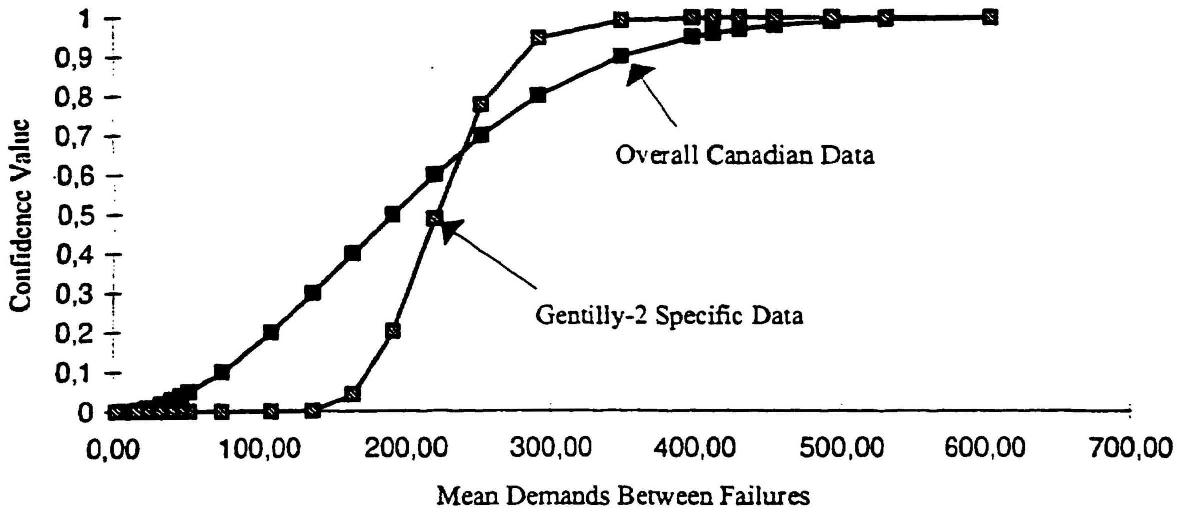

FIGURE 1. BAYESIAN UPDATING OVERALL MOTORIZED VALVE DATA

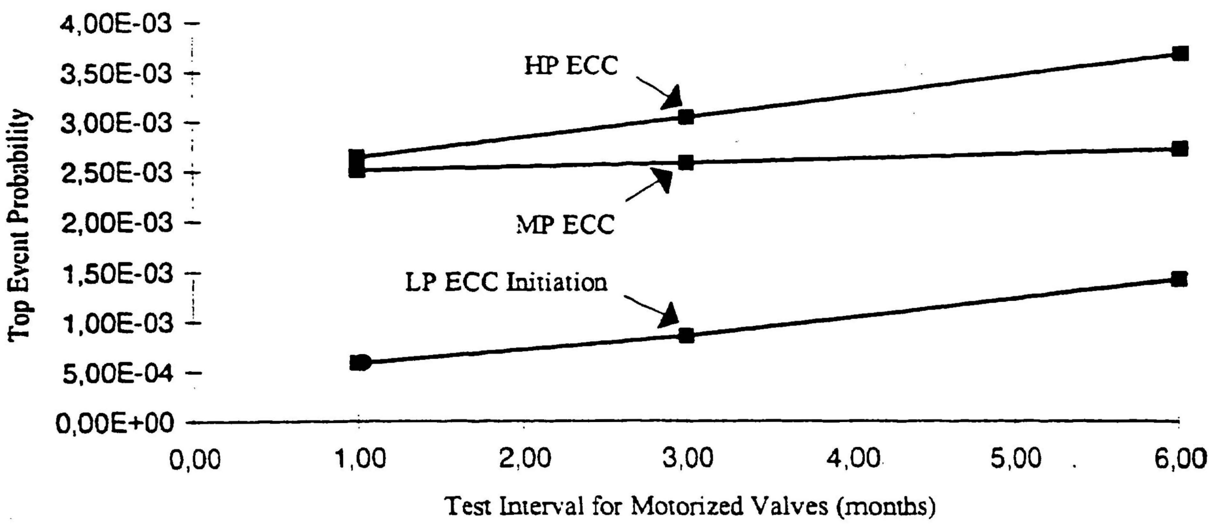

FIGURE 2. FAULT TREE RESULTS - EMERGENCY CORE COOLING