Journal of the Korean Nuclear Society
Volume 15, Number 1, March, 1983

《Original》

A Reliability Analysis of CVCS

Chung Chan Lee, Byung Soo Lee and Chang Sun Kang

Seoul National University

(Received November 20, 1982)

노냉각수 제어계통의 신뢰도해석에 관한연구

이정찬 · 이병수 · 강찬순

서울대학교

(1982. 11. 20 접수)

Abstract

The reliability of the Chemical and Volume Control System has been analyzed in a pressurized water reactor. The boration failure was taken to be the top event for this reliability analysis. A detailed fault tree was constructed and the minimal cut sets were derived. It was computed that the unavailability of the Chemical and Volume Control System due to boration failure was 1.497×10^{-5} during plant operation. It was found that the reliability of boric acid transfer pumps were the most important factors in the availability of the Chemical and Volume Control System. As expected, human errors also introduce the high system unavilability.

요 약

가압 경수로의 노 냉각수 제어계통의 신뢰도를 해석하였다. 이 신뢰도 해석에서 붕소주입실패를 상위사고로 설정하였다. 신뢰도 해석은 고장계통도를 작성한 후 이 고장 계통도로부터 최소절군을 구하였다. 붕소주입실패에 의한 노 냉각수 제어계통의 불가용성은 1.497×10^{-5}으로 계산되었다. 노 냉각수 제어계통의 불가용성에 가장 중요한 영향을 미치는 것은 붕산전달펌프의 신뢰도이며, 인간의 실수 역시 계통 신뢰도에 중요한 인자임이 나타났다.

1. Introduction

In this paper, we took the Chemical and Volume Control System(CVCS) for the reliability analysis in a pressurized water reactor. The CVCS is essential for normal operation of a pressurized water reactor. The reliability analysis of a system like CVCS could provide us with the important data for safe design and operation of a reactor. The system diagram is based on the Final Safety Analysis Report(FSAR)[1] of Korea Nuclear Unit 1. According to the Component failures at pessurized water reactor prepared by Combustion Engineering, INC.[2], the CVCS unavailability contribution to a pressurized water reactor is 0.142% per plant year. This ranks the 13th among 40 systems based upon the operating data from July 1961 through December 1978.[2] The CVCS is designed to provide various essential services to the reactor coolant system. We took the boration failure as the top event for the system definition, since the boration mode is important to the reactor safety. After deciding the top event, a detailed fault tree is constructed for a quantitative analysis of the system reliability. 'PREP'[3] code is used in this study to analyze the fault tree and obtain the minimal cut sets. The component failure intensity and fault duration time (or component unavailability) together with the minimal cut sets found by the 'PREP' become the input of 'KITT-1'[3] for this reliability analysis.

2. System Description

Among several subsystems in the CVCS, the reactor makeup control system is closely related to the reactor safety since it controls the soluble neutron absorber (boron) concentration in the reactor coolant. The reactor makeup control system is also used to maintain the proper reactor coolant inventory. In addition, for emergency boration and makeup, it can also provide refueling water to the suction of the charging pumps. The boric acid is stored in two boric acid tanks. Two boric acid transfer pumps are provided in order to transport boric acid: one pump normally aligned to the boric acid blender, and the other in reserve. On a demand signal by the reactor makeup controller, the pump switches to high speed and delivers boric acid to the boric acid blender. The pump can also be used to recirculate the boric acid tank fluid. All portions of the CVCS which normally contain concentrated boric acid solution are heat traced in order to maintain the solution temperature at 145°F. Fig. 1 describes the simplified diagram of boration mode in the CVCS.

2.1. Boration

The "borate" mode of operation permits the addition of a preselected quantity of concentrated boric acid solution at a preselected flow rate to the reactor coolant system. The operator sets the mode selection switch to "borate", the concentrated boric acid flow controller setpoint to the desired flow rate and the concentrated boric acid batch integrator to the desired quantity, and initiates the system start. This opens the makeup

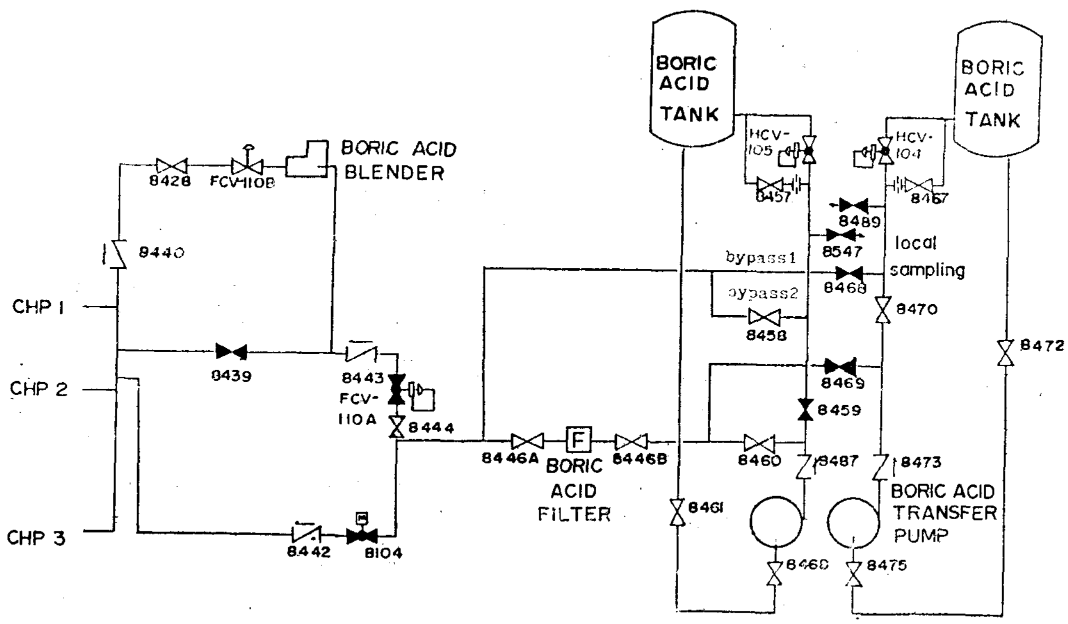


Fig. 1. Simplified Diagram of Boration System.

stop valve to the charging pump's suction, positions the boric acid flow control valve, and switches the selected boric acid transfer pump to high speed. When the preset quantity of boric acid solution is added, the batch integrator causes the makeup to stop. Also, the operation may be terminated manually at any time.

2.2. Technical Specification

To ensure safe reactor operation, technical specifications are set up for boration mode.

a. When the fuel is in the reactor there shall be at least one flow path to the core for boric acid injection.

b. The reactor shall not be made critical unless the following conditions are met:

1. two boric acid transfer pumps shall be operable,

2. at least one boric acid tank shall contain a minimum of 2,000 gallons of 11.5% to 12.5% by weight boric acid solution (20,000ppm to 21,900ppm boron) at a temperature of at least 145°F,

3. system piping, instrumentation, controls, and valves shall be operable to the extent of establishing one flow path from the refueling water storage tank to the reactor coolant system, and

4. two channels of heat tracing shall be operable for the above flow paths for concentrated boric acid.

c. During power operation, the requirements of the above paragraph b may be modified to allow any one of the following components to be inoperable:

1. one channel of the heat tracing may be out of service provided it is restored to operable status within 48 hours, and

2. one boric acid transfer pump may be out of service provided both pumps are again operable within 24 hours.

If the system is not restored to meet the requirements of paragraph b within the time period specified, the reactor shall be placed in the hot shutdown condition utilizing normal operating procedures. If the requirements of paragraph b are not satisfied within an additional 48 hours, the reactor shall be placed in the cold shutdown condition utilizing normal operating procedures.

2.3. Fault Tree Construction

The failure of boration in the CVCS is chosen as the top event in the fault tree construction. The boration system includes the components starting from boric acid tanks to the charging pump suction header as shown in Fig. 1. Since we were interested in the boration failure itself under normal operating condition, when constructing the fault tree, we neglected the failure modes which might be caused by exceeding the design limit of each component, and the primary events were restricted to the component levels and not further down. The fault tree constructed for unavailability calculation is presented in Fig. 2. The fault tree structure for the failure of boration is very similar to that for unavailability calculation. When constructing such a fault tree, it is assumed that all components are in the functioning state at time $t=0$ and two boric acid transfer pumps are in the operating state. Since the bypass lines are available, bypass lines 1 and 2 are also assumed to be open. Human errors and command signal failures after the demand of boration are not considered.

3. Reliability

There are two general system requirements for quantification in the reliability analysis. The first requirement is that a system be available upon demand when the initiating event occurs. The probability that a given system is not available upon demand is usually defined as its unavailability. The unavailability of a system is comprised of failure contributions which both

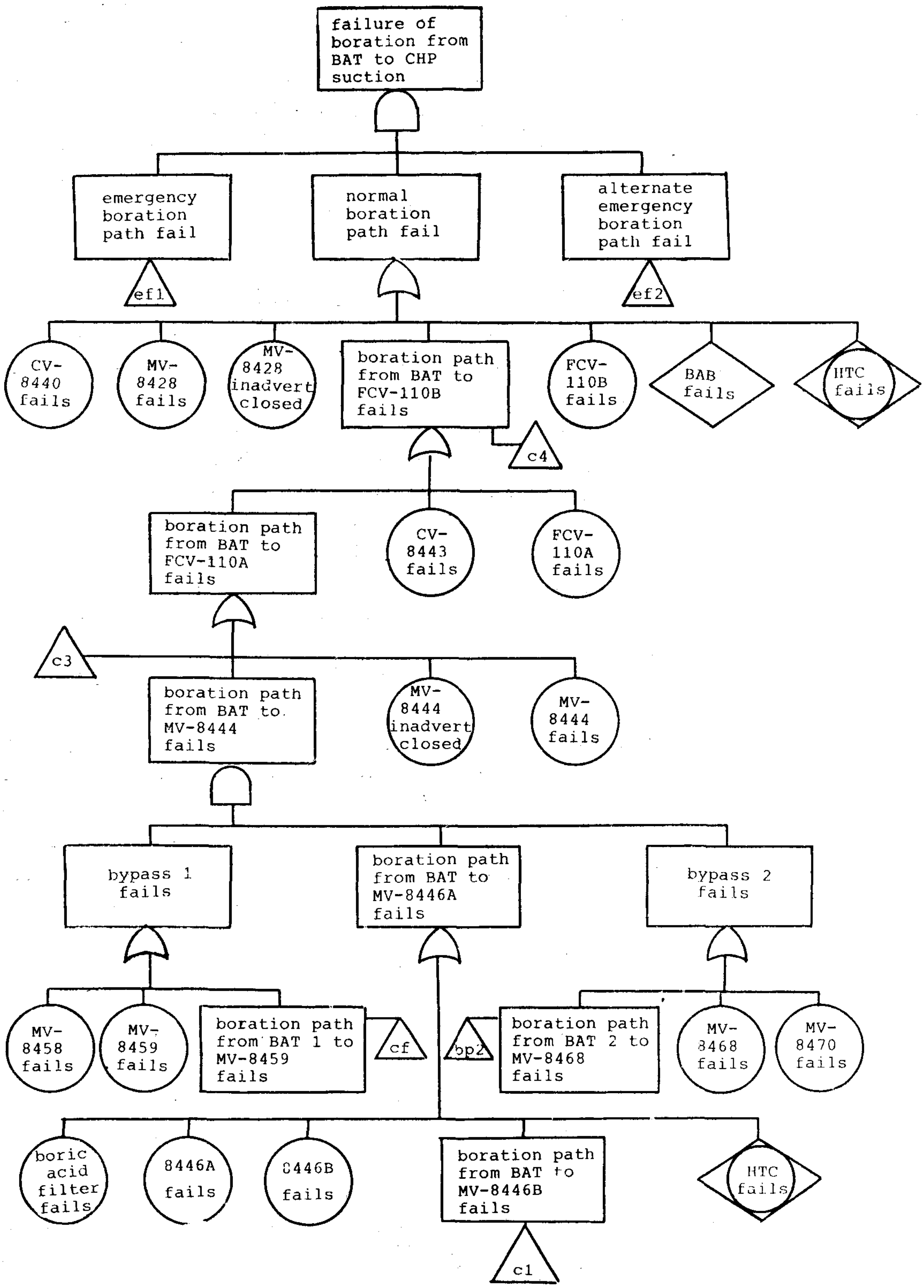
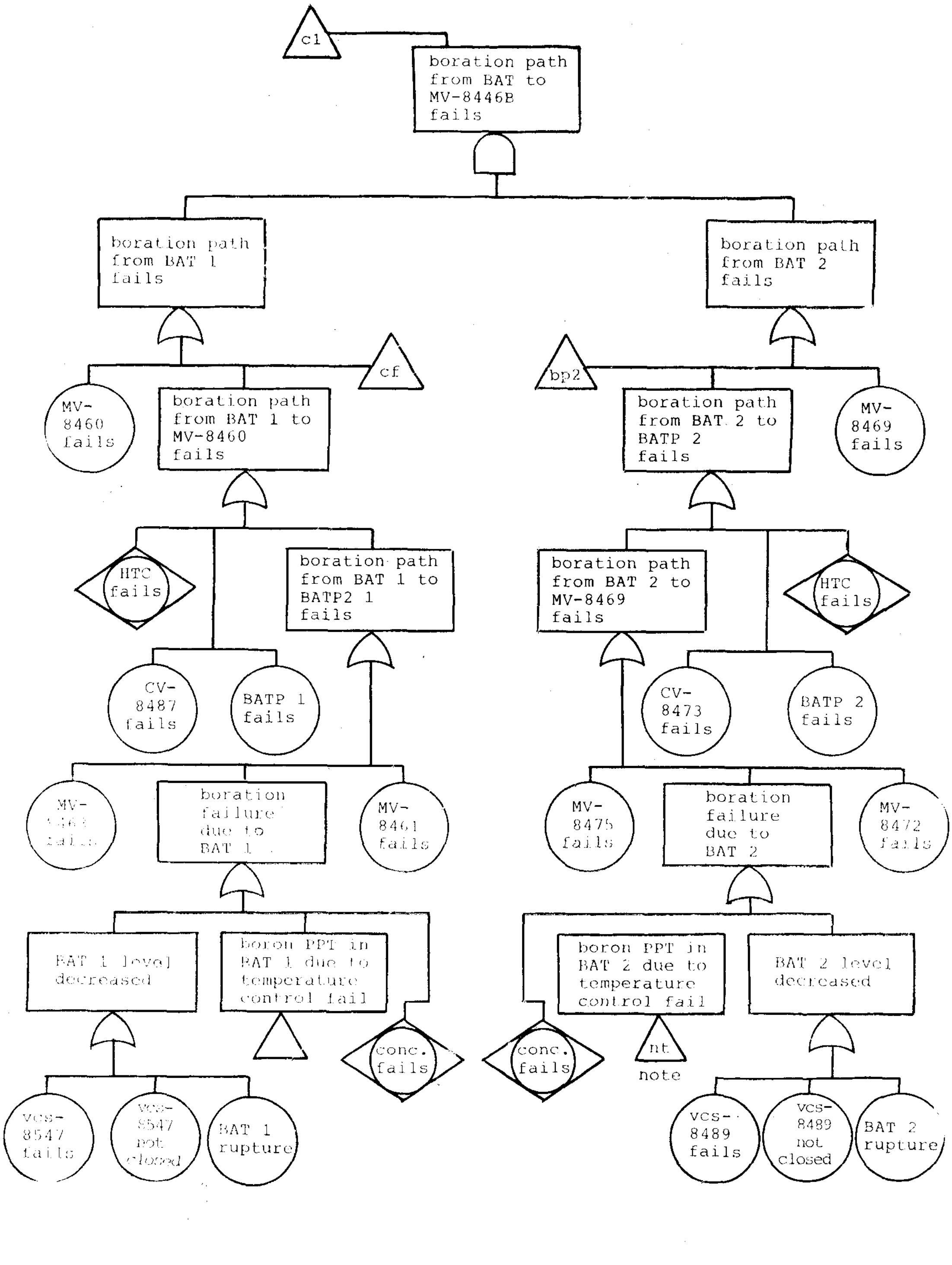
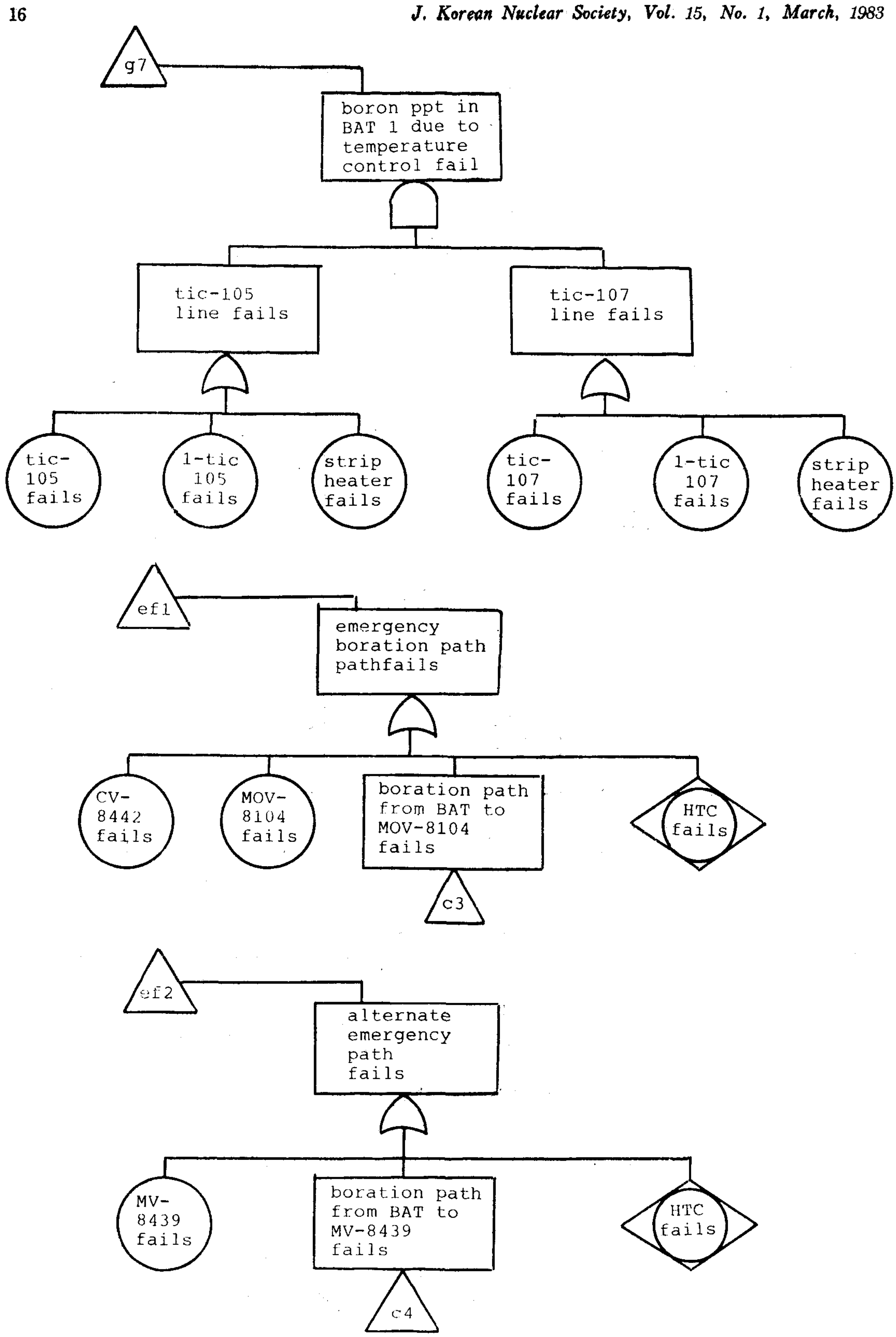


Fig. 2. Standby State Boration System Fault Tree



note: nt subtree has same structure as that of g7.


g7
boron ppt in BAT 1 due to temperature control fail
tic-105 line fails
tic-107 line fails
tic-105 fails
1-tic 105 fails
strip heater fails
tic-107 fails
1-tic 107 fails
strip heater fails
ef1
emergency boration path pathfails
CV-8442 fails
MOV-8104 fails
boration path from BAT to MOV-8104 fails
HTC fails
c3
ef2
alternate emergency path fails
MV-8439 fails
boration path from BAT to MV-8439 fails
HTC fails
c4

originates prior to the actual demand (e.g., undetected component failures, maintenance contributions, etc.) and occurs at the time of demand (e.g., system realignment failures and starup failures). The second requirement is that a system operates for its necessary period of time following the initiating event. The probability for unsuccessful operation is defined as the system failure probability. The failure probability depends on the length of time the system must function, and is affected by the operational schemes employed. With these basic considerations, the fault trees were constructed, and system unavailability and failure probability were quantified. The total system failure probability is the sum of the two contributions: unavailability and system failure probability.

3.1 Reliability of Standby Systems

3.1.1 Component Unavailability

For those components that are required to start, change state, or function, the probability that the component will fail to operate upon demand is called as the demand probability. The demand probability incorporates the contributions failure at demand, failure upon demand, as failure to continue operation for a sufficient period of time for successful response to the need. Component unavailability can be expressed by failure intensity and demand probability. For nonrepairable components, unavailability Q can be expressed as follows:

$$Q=\frac{1}{2}\lambda T \tag{1}$$

where T is the test interval, and λ is the failure intensity. For monitored components, unavailability Q is given by the following equation:

$$Q=\lambda\tau \tag{2}$$

where τ is the fault duration time. In case that the success or failure of a component can be determined if there exists a demand, Q can be given by the formula,

$$Q=q_d+\lambda\tau \tag{3}$$

where q_d is the demand probability.

System Unavailability

Let Q_0 be the system unavailability, then

$$Q_0=Q_1-Q_2+Q_3-Q_4+\cdots+(-1)^{N_c-1}Q_{N_c} \tag{4}$$

and

$$Q_0\leqq 1-\prod_{i=1}^{N_c}(1-\check{Q}_i) \tag{5}$$

where Q_n is the probability that n minimal cut sets are unavailable simultaneously, N_c is the total number of minimal cut sets and $\check{Q}_i$ is the unavailability of the minimal cut set i.[4] We can take the right hand side of the above seond equation as the upper bound of the system unavailability. Since the average component failed probability is much less than one and the order of Q_2 is about twice as small as that of Q_1, the contribution of Q_n is negligible if n is greater than or equal to two. In this analysis the upper bound approximation is used for Q_0 rather than Q_1 approximation. This is because the upper bound approximation is true as long as the cut sets are independent.

3.2 Time Dependent Reliability

Relability is a characteristic of an item expressed by the probability that it will perform its function or functions in the desired manner during the time period from the start of its operation to a time t. The time dependent calculation of reliability is performed with the KITT-1 code that uses a so-called Kinetic Tree Theory.[4] In this code, components are assumed in the functioning state at time $t=0$. It is also assumed in the code that failure intensity λ for every component is constant with respect to time. It further assumes that each component has a constant repair time. The cumulative probability of failure, FSUM is given by[3)4)]

FSUM=

$$1-\exp\left\{-\int_0^t\left[\frac{\sum_{i=1}^{N_c}\check{W}_i(t')}{\prod_{i=1}^{N_c}[1-\check{Q}_i(t')]}\right]dt'\right\} \tag{6}$$

where $\check{Q}_i(t)$ is the probability that minimal cut set i is in its failed state at time t, and $\check{W}_i(t)$ is the failure of minimal cut set i at t, i.e., the probability that failure of the system (or component) will occur at time t per unit time.

3.3 Unavailability Data

The unavailability data of each component is presented in Table 1. Pipes are neglected since they are considered passive systems with very low failure intensity.

The values in Table 1 were obtained as follows:

a. The probability of leaving a manual valve open after checking boric acid concentration is 1.0×10^{-2}, the maximum fault duration time is one week, then the unavailability comes (1.0×10^{-2}) $(7/365)=1.92\times10^{-4}$. This unavailability is rather overestimated since we neglet the level indicators and alarm system.

b. A boric acid transfer pump operates at high speed in the boration mode. So the unavailability of the boric acid transfer pump is the sum of the unavailabilities of switching to high speed $q_d=1\times10^{-3}$ and since the boric acid transfer pump should be repaired within 24 hours, running for 24 hours ($\lambda_0=3\times10^{-5}$/hr, τ=24hrs), and of maintenance q_m. The test of boric acid transfer pumps is carried out during refueling period, hence no test induced downtime is considered. Non-routine maintenance ranges from monthly to yearly with a mean pump maintenance interval of 4.5 months/act or a mean frequency, f, of maintenace of 0.22 acts/month. The maintenance contribution to unavailability q_m is given by the equation

$$q_m=f\times t_d/720,$$

when t_d is now the average maintenace downtime, and the average downtime due to maintenance is seven hours.[5] Then the unavailability of a boric acid transfer pump becomes 3.86×10^{-3}. However it should be noted that simultaneous maintenance of the two pumps cannot be performed.

c. The failure mode of check valve CV8473 is rupture, or internal leak.

d. The failure mode of normally closed manual valve are plugging and rupture. The probability of plugging is the demand probability of $q_d=1.0\times10^{-4}$, and rupture can be expressed by failure intensity.

e. Internal leak, failure to open and rupture consist in the failure modes of check valve CV8443. The failure intensities of internal leak and rupture are: $\lambda_0=3\times10^{-7}$/hr, and $\lambda_s=1.0\times10^{-8}$/hr. The demand probability is: $q_d=1.0\times10^{-4}$.

f. Pneumatic valves can be failed in the following modes: failure to open on command: $q_d=3\times10^{-4}$, rupture: $\lambda=1\times10^{-8}$/hr, τ=84hrs, and plugged: $q_d=3\times10^{-4}$ Hence the sum becomes: $q_{sum}=4.0084\times10^{-4}$.

g. The failure probability of heat tracing is obtained from a fault tree in Safety Study Appendix II Chapter 5.[5]

h. These two valves are located where no circulating boric acid flow is. Human error to close a valve inadvertently cannot be found until the system requires it to remain open, so this kind of human error can be included.

i. 24 hour limit fault duration time is specified for some important components and use of 24 hour limit as an upper bound gives a mean duration of seven hours. Since there is no fault duration data available for other components, they are assumed conservatively to be checked once a week. Hence 84 fault duration time comes out. But in actual plant, routine check for important components and subsytems is performed, and we can introduce seven hour fault duration time.

j. Boric acid filter is checked once a week. Its failure mode consists of leakage and blockage with failure intensity of 1.0×10^{-6}/hr.[6]

Table 2 shows the failure modes and intensities of components in the CVCS.

All the above data [illegible] from APP. III of WASH-1400[5].

Table 1. Failure Data Related to the Demand and Standby State

basic event	failure intensity, Hr^{-1}	fault duration time, Hr^{i}	unavaila-bility, q	ref.
TIC104	3E-6	84	2.52E-4	9
1-TIC104	4.07E-6	84	3.42E-4	9
HEATERD	3.56E-6	84	2.99E-4	9
TIC103	3E-6	84	2.52E-4	9
HEATERC	3.56E-6	84	2.99E-4	9
VCS8439	1E-8	84	8.40E-7	5
BATBRUP	1E-9	84	8.40E-8	5
TIC107	3E-6	84	2.52E-4	9
1-TIC107	4.07E-6	84	3.42E-4	9
HEATERB	3.56E-6	84	2.99E-4	9
TIC105	3E-6	84	2.52E-4	9
1-TIC105	4.07E-6	84	3.42E-4	9
HEATERA	3.56E-6	84	2.99E-4	9
VCS8547	1E-8	84	8.40E-7	5
BATARUP	1E-9	84	8.40E-8	5
BATCONB[a]			1.92E-4	5
MV8475	1E-8	84	8.40E-7	5
MV8472	1E-8	84	8.40E-7	5
BATP2[b]			3.86E-3	5
CV8473[c]	3.10E-7	84	2.604E-5	5
MV8469[d]			1.0084E-4	5
BATCONA[a]			1.92E-4	5
MV8463	1E-8	84	8.40E-7	5
1-TIC103	4.07E-6	84	3.42E-4	9
MV8461	1E-8	84	8.40E-7	5
BATP1[b]			3.86E-3	5
CV8487	3.10E-7	84	2.604E-5	5
MV8460	1E-8	84	8.40E-7	5
BAFILTER[j]	2E-6	7	1.40E-5	6
MV8446B	1E-8	84	8.40E-7	5
MV8446A	1E-8	84	8.40E-7	5
MV8468			1.0084E-4	5
MV8458	1E-8	84	8.40E-	5
MV8444[d]			1.0084E-4	5
CV8443[e]			1.2604E-4	5
FCV110A[f]			4.0084E-4	5
HTC1[g]	6.23E-7	7	4.36E-6	5
CV8440	1E-8	84	8.40E-7	5
MV8428			1.438E-4	5
FCV110B[f]			4.0084E-4	5
BAB			3.00E-4	5
MV8439			1.438E-4	5
HTC3[g]	6.23E-7	7	4.36E-6	5
[illegible]442			1.46E-4	5
[illegible]	6.23E-7	7	4.36E-6	5
MOV			1.1008E-3	5
HTC4[g]	6.23E-7	7	4.36E-6	5
HTC5[g]	6.23E-7	7	4'36E-6	5
HTC6[g]	6.23E-7	7	4.36E-6	5
H8428[h]			3.00E-4	5
H8444[h]			3.00E-4	5
H8547[a]			1.92E-4	5
H8489[a]			1.92E-4	5
MV8459[d]			1.0084E-4	5
MV8470	1E-8	84	8.40E-7	5

Abbreviations

TIC : Temperature Indicator
1-TIC : Temperature Controller
HEATER : Electric Heater
BATRUP : Boric Acid Tank Rupture
MV : Manual Valve
CV : Check Valve
BATP : Boric Acid Transfer Pump
BAFILTER: Boric Acid Filter
FCV : Flow Control Valve
HTC : Heat Tracing Channel
BAB : Boric Acid Blender
MOV : Motor Operated Valve
H : Human Error
BATCON : Boric Acid Concentration Failure

4. Result and Conclusions

4.1. Unavailability upon Demand of Boration

The results of unavailability calculation on boration demand are summarized in Table 3. For the purpose of comparison, Table 3 presents the results without pump maintenance as well as with maintenance. From the results, one can find out the conservative system unavailability, 1.470×10^{-5}. As the unavailability of the boric acid transfer pump increases, the increase of fault duration time does not affect the system unavailability significantly. This is because the unavailabilities in an operating state are comparatively smaller than the demand unavailabilities. The minimal cut sets important to the system unavailability were chosen from about

Table 2. Failure Modes and Failure Intensity Related to the Operating State

Component	Failure Mode	Failure Intensity(hr^{-1})
boric acid transfer pump	failure to run	3.00×10^{-5}
manual	valve rupture	1.00×10^{-8}
check valve	plugged or rupture	3.10×10^{-7}
temperature indicator	failure to indicate temperature	3.00×10^{-6}
heat tracing channel	failure to maintain appropriate temperature	6.23×10^{-7}
motor operated valve	rupture or failure to remain open	3.10×10^{-7}
temperature controller	failure to control temperature	4.07×10^{-6}
pneumatic value	rupture or failure to remain open	3.10×10^{-7}
heater	failure to heat	3.56×10^{-6}
boric acid filter	leakage or blockage	2.00×10^{-6}

150 minimal cut sets according to their importance ranking. The nine important minimal cut sets which is shown in Table 4 actually contributes about 97 percent of the system unavailability. Among these minimal cut sets, the simultaneous failure of two boric acid transfer pumps is the largest factor in this system unavailability. In most cases, the other minimal cut sets also contain the failure of a boric acid transfer pump. This is because the unavailabilcability of a boric acid transfer pump is larger than those of any other components. Besides the unavailability of boric acid transfer pumps, human error is also important. Among the nine minimal cut sets given in Table 4, five minimal cut sets involve with human errors and their combined unavailability is 3.28×10^{-6} that is about 22.3 percent of the system unavailability. The five basic events associated with human errors are BATCONA, BATCONB, H8489, H8547, and H8444. In fact, since the test and maintenance should be performed according to the given operating and maintenance procedures, and some valves have lock systems in order to prevent inadvertent human errorshuman error contribution to the system is rather highly overestimated. However human error should be fully considered when it is related to the routine work.[7]

4.2. Reliability during Boration

45 minimal cut sets of order two were obtained by the deterministic method, COMBO subroutine, of PREP code. Among these minimal cut sets the important minimal cut sets are those which include boric acid transfer pump numbers 1 or 2. These cut sets contribute 94 percent to the system reliability during boration. The minimal cut sets of order three found by the Monte Carlo method, FATE subroutine of PREP code, consist of temperature controller, indicators, strip heaters in the boric acid tanks, heat tracing channel and boric acid transfer pumps.

In Fig. 3, the cumulative failure probability is shown for the first 24 hours of boration, which rapidly increases as an exponential function. In Fig. 4, it is shown that the system failure intensity[3,4] is expressed as a time dependent

Table 3. Unavailability of Boration of the CVCS

	fault duration time(hr)	upper bound	lower bound
with	84	1.470×10^{-5}	1.470×10^{-5}
pump maintenance	7	1.446×10^{-5}	1.445×10^{-5}
without	84	5.462×10^{-6}	5.460×10^{-6}
pump maintenance	7	4.695×10^{-6}	4.693×10^{-6}

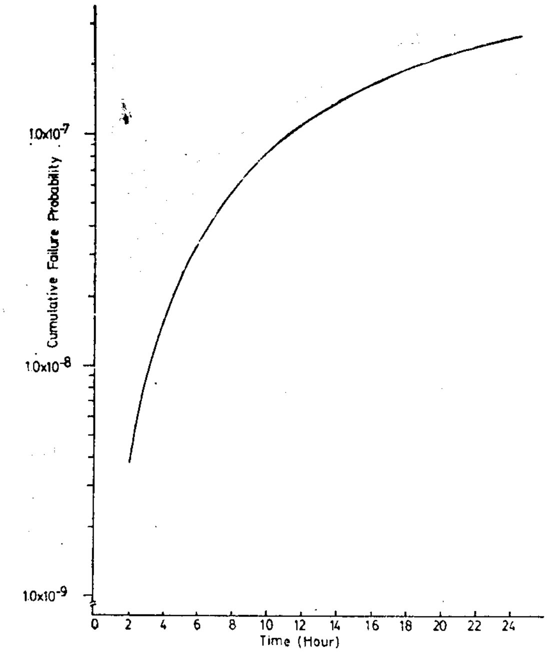


Fig. 3. System Cumulative Failure Probability

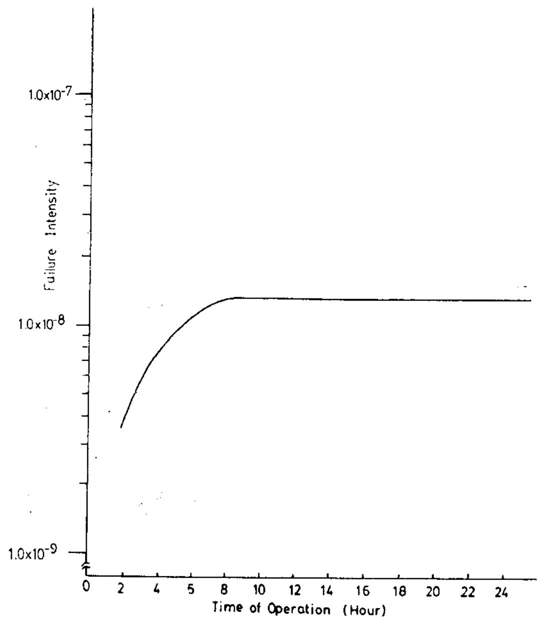


Fig. 4. System Failure Intensity

function. It increases rapidly until the time reaches six to eight hours and then saturates. In other words, if the system is operable at time t, the system failure probability is the same at

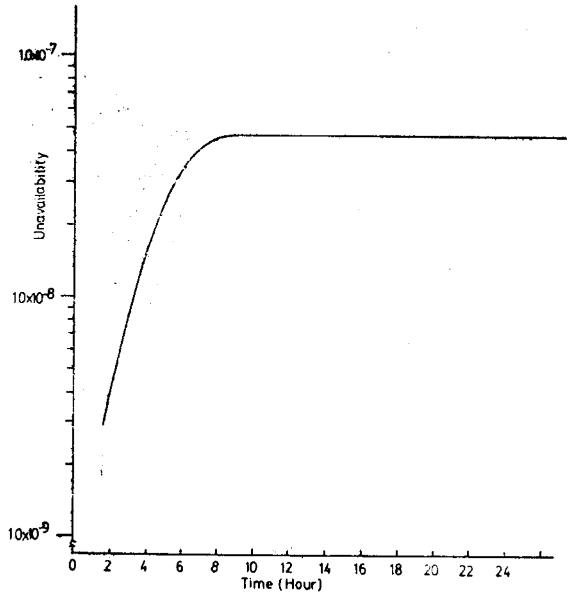


Fig. 5. System Unavaility

time t and at time $t+dt$ following six to eight hour operation.[6,8] Since the boration mode is not always used, the reliability during operation is rather important than its unavailability, i.e., it is important that is performs its mission successfully until a certain time t. At time t, the unavailability which means that the system is in a failed state reaches the maximum value of 4.7×10^{-8} at eight hour following the operation and then it maintains the plateau. It is illustrated in Fig. 5. In actual boration mode, time dependent reliability characteristics during the initial three hours[1] well represent the boration system failure probability and unavailability.

4. 3. Conclusion

The unavailability of boration in the CVCS at the standby state is calculated to be 1.470×10^{-5}, and the cumulative failure probability becomes 2.743×10^{-7} at the 24 hour mission period. Hence the unavailability of boration becomes 1.497×10^{-5}. The basic events and components which significantly affect the system reliability are two boric acid transfer pumps, human error, motor operated and pneumatic valves. Among them, two boric acid transfer pumps significantly affect the system unavailability, and need higher quality in order to improve the system reliability. The other improvement should be the reduction of the human causing unavailabilty by using the certified form of procedures or by employing competent and redundant persons.

Table 4. Important Minimal Cut Sets and their Unavailabilities

minimal cut sets	unavailability
BATCONA, BATP2	7.4112×10^{-7}
BATP1, BATCONB	7.4112×10^{-7}
BATP1, BATP2	1.0325×10^{-5}
BATP1, CV8473	1.0051×10^{-7}
CV8487, BATP2	1.0051×10^{-7}
MOV, FCV110A	4.4126×10^{-7}
BATP2, H8547	7.4112×10^{-7}
BATP1, H8489	7.4112×10^{-7}
MOV, H8444	3.3024×10^{-7}
sum $=1.4262\times10^{-5}$	

Acknowledgements

The authors would like to thank Korea Science and Engineering Fund for its financial aid. Thanks are also due to Dr. Won Guk Hwang of the Korea Advanced Energy Research Institute for providing useful informations.

References

1. "Final Safety Analysis Report," for Ko-ri Nuclear Power Plant Unit No. 1, KECO, 1977.
2. "Component Failures at Pressurized Water Reactors," Final Report, Combustion Engineering, INC., Nuclear Power Systems, ALO-74, 1980.
3. W.E. Vesely and R.E. Narum, "PREP and KITT: Computer Codes for the Automatic Evaluation of a Fault Tree," IN-1349, Aug., 1970.
4. W.E. Vesely, "Analysis of Fault Trees by Kinetic Tree Theory," IN-1330, 1969.
5. Nuclear Regulatory Commission, "Reactor Safety Study-An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," NRC Robert WASH-1400 (NUREG-75/104), NTIS, Oct., 1975.
6) A.E. Green, "Reliability Technology," London, Wiley, 1972.
7. H. Kragt, "Human Reliability Engineering," IEEE trans. on Reliability, vol. R-27, No. 3, Aug., 1978.
8. M.L. Shooman, "Probabilistic Reliability in Engineering Approach," McGraw-Hill, 1968.
9. "IEEE Guide to the Collection and Presentation of Electrical, Electronics, and Sensing Compoent Reliability Data for Nuclear-Power Generating Stations," IEEE std 500-1977, 1977.