OPTIMIZATION OF FAULT TREE ANALYSIS USING THE FACTORIAL DESIGN APPROACH

by

M.L. YAMPOLSKY
POLAROID CORPORATION

J. A. ADAM
P. KARAHALIOS
STONE & WEBSTER
ENGINEERING CORPORATION

Presented at
AICHE SUMMER
NATIONAL MEETING
Seattle, Washington
August 25-28, 1985

TP 85-26
NX/CSG

STONE & WEBSTER ENGINEERING CORPORATION
BOSTON, MASSACHUSETTS

OPTIMIZATION OF FAULT TREE ANALYSIS USING THE FACTORIAL DESIGN APPROACH

Marina L. Yampolsky
Polaroid Corporation
Cambridge, MA

James A. Adam
Stone & Webster Engineering Corporation
Boston, MA

Paris Karahalios
Stone & Webster Engineering Corporation
Boston, MA

ABSTRACT

An application of orthogonal factorial design (OFD) to supplement fault tree analysis (FTA) is presented. The combination of OFD and FTA permits mathematical evaluation of relative contributions of single events to system reliability. The approach permits detection of potential weaknesses in the design stage and determination of the most effective means of optimization.

BACKGROUND

Fault tree analysis (FTA) is a systematic and logical procedure to study and analyze complex systems for undesired events and their causes. It has many applications for determining system reliability and availability. Principles and computer codes for FTA are well developed and easy to implement, and the analysis can be extended to either the system or component level.

When used alone, however, FTA is confined to general information about the system. This information usually includes minimal cutsets, availability, etc., when such codes as KITT or SUPKITT are used. Results from such analysis have a high level of uncertainty because of the subjectivity of the input data.

The input into fault tree quantitative analysis is failure rate data on components or subsystems, and the top event, reliability or availability, is evaluated based on this information.

There are several problems related to using failure rate data. First, all fault tree quantitative codes are based on the assumption that the failure rate values are constant. Some components, however, exhibit strong wearout phenomena. Also, failure rate data for particular components are limited, so analysts must rely on the subjective approach of using data for "similar components." Some data, such as data on operating chemical plants, are broadly "lumped" together and much too general. Another problem is that increasing failure rates due to environmental effects (i.e., temperature or humidity) may deteriorate component performance to some unknown degree. System reliability also may be effected dramatically through unidentified subsystem or component interactions([1]) (e.g., when an effect caused by a change in some component state may change the effect of other components on the total system performance). These "hidden" interactions cannot be estimated through ordinary FTA. Because of these uncertainties, output from the FTA cannot be used alone as a reliable design basis. However, efforts can be made during the design stage to reduce these uncertainties and to help in system optimization.

Design decisions can be made with less uncertainty and more objectivity if mathematical relationships are established between component or systems states and top events. Analyzing these relationships will provide insight into system availability and guide the designer in selecting remedies at minimum cost. Evaluation based on mathematical relationships of the results will identify components and subsystems that have maximum impact on system or plant availability. Steps can then be taken to either replace such components or modify the design with minimal cost impact.

The following technique is suggested as a supplement to FTA to allow establishment and evaluation of the mathematical relationships between the top event and components. The relative importance of components is estimated using this technique, and such "importance rank" becomes the criterion for the design rather than absolute failure rates. This approach helps identify the most critical components and provides a basis for design decisions (i.e., where redundancy is needed, which portion of the design needs improvement, etc.). Also, certain types of interactions within the system are estimated along with their effects on system availability. Only relative values of failure rates are needed for the analysis, significantly reducing the uncertainties and enabling the analyst to evaluate the system sensitivity within the broad limits of subsystems/components failure rates.

PROPOSED METHODOLOGY

The proposed methodology is a combination of FTA with orthogonal factorial design (OFD). Combining these two techniques enables an analyst to benefit from using FTA, while overcoming its most

significant drawback--lack of meaningful and formalized information about the relative contributions of components to total system (plant) reliability.

This new approach modifies the computerized fault tree assumption that component characteristics (such as failure probabilities) remain unchanged over the life of the plant. Instead, this method assumes that failures (or availability rates) for components in the fault tree structure vary randomly with time over an established range.

The input data necessary to obtain quantitative characteristics from FTA are the component failure rates. Failure rates may be constant or may vary with respect to phasing, in accordance with some assumed distribution. Each change in the failure rate requires a new computer run. Thus, the fault tree is evaluated in many stages, resulting in probability characteristics that are difficult to analyze. Each result will be evaluated for the given "fixed" failure rate, and all other intermediate states of the component still will be beyond the analysis.

As previously mentioned, the availability of a component may vary under the effects of temperature, humidity, etc. Sources such as IEEE, NERC, and other industry data banks for component failure rates may be used for preliminary information. Use of the OFD approach allows the introduction of component failure rate variations in the fault tree structure in a way that results in meaningful analysis and conclusions.

OFD can be viewed as a series of experiments (in this case, computer solutions to the fault tree quantification) in an effort to develop a simplified prediction model of system availability (similar to regression analysis). The series of experiments is designed beforehand to--

- Minimize the number of trials
- Optimize model accuracy
- Provide detailed system/component relationships

Generally, each computer evaluation results in the system availability (response) based on a set of discrete failure rates for each component (levels). For each fault tree quantification, the levels of each variable are chosen according to OFD, to provide independence in estimating the effects of each variable. The resultant series of computer evaluations is a matrix of variable levels with columns orthogonal to each other.

Mutual independence is the most important feature of this technique because calculated regression coefficients for each variable reflect the effect of only that variable on the system response. Furthermore, the combination of the orthogonal vectors is designed

to optimize input/output mathematical relationships by minimizing errors in the evaluation of single effects within the range of values chosen for each variable. For example, in studying the effects of a component with failure rates from -1 to +1 (coded level for minimum failure rate to coded level for maximum failure rate) on a system that is effected by a total of n components, the (n+1)th-dimensional response surface that results from the analysis reflects all possible effects of the component under study for all combinations of other component failure rates. A typical orthogonal matrix for five components is presented in Table 1.

APPLICATION OF OFD TO FTA

First, the plant or system fault tree is constructed and component failure rates are compiled. Then uncertainty bounds for the collected failure rates are used to establish maximum and minimum failure rates for each component (coded values of +1 and -1). If uncertainty bounds are not readily available, then engineering judgment can be used to establish them. These different levels of failure rates are arranged in an orthogonal matrix (see Table 1).

Computer runs are performed to quantify the fault tree (failure rates) using input data in accordance with the orthogonal matrix. Analysis of the results of the fault tree quantification for the top event failure probability, availability or unavailability Q(u) is performed in orthogonal factorial analysis by first writing a relationship between the components and the top event as a polynomial with "n" variables.

$$Q(u) = C_0 + C_1X_1 + \ldots C_iX_i + \ldots C_nX_n + C_{ii}X_i^2 + \ldots C_{jj}X_j^2 + \ldots C_{nn}X_n^2 + C_{12}X_1X_2 + C_{ij}X_iX_j + \ldots C_{ij\ldots n}X_iX_j\ldots X_n \quad (1)$$

where:

The variables $X_1, \ldots X_i, \ldots X_n$ represent the subsystems (components) included in the FTA and are expressed numerically in terms of failure rates in the normalized form.

$X_1X_2, \ldots X_iX_j, \ldots X_iX_j \ldots X_n$ = interactions among subsystems (components) failures.

$C_0, C_1, \ldots C_n; C_{11}, \ldots C_{ii} \ldots C_{nn}$ = coefficients of regression for linear and quadratic effects, respectively, or the main effects according to the established terminology.

$C_{12},\ldots C_{ij},\ldots C_{ij}\ldots n$ = coefficient of regression for two or more variable interaction effects.

When the number of components in the fault tree is large, the total number of failure rate combinations becomes enormous. Without representing results in the polynomial form (Equation 1) the study tends to be complicated, and the results do not clearly reflect the effect of individual components on system availability.

If the top event availability is evaluated under fixed conditions, e.g., fixed component failure rate, this interpretation of the results would lack flexibility and may lead to decisions that could jeopardize plant safety or operation.

A simulation using OFD will give a simple form of an approximate equation. If independence in the evaluation of the coefficient in the equation is provided, the value of each coefficient will reflect the actual effect of the corresponding variable (component state): the larger the coefficient of a variable, the greater the effect of this component.

Mathematically, this means all columns in the matrix of variables X (F_x) are mutually independent, or F_x is the orthogonal matrix. The theoretical aspects of constructing the orthogonal matrices were developed by Addelman[2,4].

The main concepts are as follows: If the regression coefficients are considered as a vector of unknown parameters

$$C = \begin{vmatrix} C_0 \\ C_1 \\ C_2 \\ . \\ . \\ . \\ . \\ C_n \end{vmatrix} \qquad (2)$$

and system failure rate or unavailability as a response vector

$$Q(u) = \begin{vmatrix} Q_0(u) \\ Q_1(u) \\ Q_2(u) \\ . \\ . \\ . \\ . \\ Q_n(u) \end{vmatrix} \qquad (3)$$

then the coefficients "C," according to the general rule of matrix algebra, are estimated as:

$$C = (F_x^T F_x)^{-1} F_x^T Q(u) \tag{4}$$

where:

F_x is n by m matrix of independent variables "X" in normalized form:

$$F_x = \begin{Vmatrix} f_1(\chi_{11},\ldots,\chi_{m1}),\ldots f_k(\chi_{12}\ldots,\chi_{m1}) \\ f_1(\chi_{12},\ldots,\chi_{m12}),\ldots f_k(\chi_{12},\ldots,\chi_{m2}) \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ f_1(\chi_{1n},\ldots,\chi_{mn}),\ldots f_k(\chi_{1n},\ldots,\chi_{mn}) \end{Vmatrix} \tag{5}$$

where:

$f_k(\chi_{1n},\ldots,\chi_{mn})$ = value of the $k^{\underline{th}}$ function of variables on $n^{\underline{th}}$ point of the matrix "F"

m = number of variables

n = number of lines in matrix F_x

F_x^T = transposed matrix of F_x.

Construction of the matrix F_x is the most critical part of the analysis because the type and size of this matrix define the accuracy of the model and number of runs required.

The orthogonality condition is met through the requirement of the matrix that moments $F_x^T F_x$ be diagonal. Currently, the procedures for designing orthogonal matrices with minimal number of lines (in our case, with minimal number of computer runs for evaluation of the top event unavailability) are well developed ([2],[3],[4],). For the analyst familiar with this technique, the design of the most economical and efficient matrix for each particular case presents no special problems. The number of variables used has no limit. Also, the orthogonal design allows simplification of the general expression for evaluation of the coefficients. Instead, the following relationships are used:

for single variables:

$$C_i = \frac{\sum_{u=1}^{N} f(\chi_i) \cdot Q(u)}{\sum_{u=1}^{N} \left[f(\chi_i) \right]^2} \qquad (6)$$

for interactions:

$$C_{ij\cdots n} = \frac{\sum_{u=1}^{N} f(\chi_i\ \chi_j\ \cdots\ \chi_n)\ Q(u)}{\sum_{u=1}^{n} \left[f(\chi_i\ \chi_j\ \cdots\ \chi_n) \right]^2} \qquad (7)$$

where:

Q(u) = value of the system availability at the combination "χ" corresponding to the u^{th} point of the matrix F_x.

Any computer code that is generally used for quantitative evaluation of system availability (e.g., KITT) may be used to estimate the numerical values of Q(u). The code must be run a limited number of times, equal to the number of lines "n" in the matrix F_x and conditions for each run are defined by the combination of "x" in the matrix F_x.

The subsequent analysis of results is straightforward: the value of C_i for any single variable reflects the quantitative effect of the corresponding component or subsystem on total availability. The higher the value of C_i, the greater the effect of the component state on Q(u) and, therefore, stronger requirements of the quality of this component and more accurate data for failure rates must be used. The same is applied to the analysis of the interactions. Significant values for the coefficients $C_{ij\ldots n}$ is evidence that there is a presence of interactions between components i, j,...n, and design decisions should be focused on the reduction of the effect of these interactions, probably through redundancy.

The relative sum of the coefficient of these interactions

$$\sum_{u=1}^{N} \left[F(\chi_{ij\cdots n}) \right] \qquad (8)$$

$$i \neq j \neq n$$

may serve as a useful criterion of system or plant effectiveness, especially for discriminatory decisions among alternative designs.

Example

The example used to illustrate this application of factorial analysis is taken from a system interaction study performed for Teollisuuden Voima Oy (TVO), Finland, on the fuel pool cooling and fuel pool purification systems of their KPA-Store (independent spent fuel facility).

The physical situation is that spent nuclear fuel rods (assemblies) will be stored underwater in vertical racks in a series of stainless steel-lined pools (Figure 1). The purpose of the facility is to maintain control over the fuel and any radioactive material associated with them until after the nuclear power plant has ceased operation and an ultimate final high level waste respository is ready (approximately 60 years).

In exercising control, the primary process operation is the removal from the fuel assemblies of decay heat which is created by the fission products. The water pools accomplish this function in conjunction with redundant closed and open cycle cooling circuits. As long as decay heat is removed, the fuel is in a safe, stable configuration. If heat cannot be removed, the fuel eventually will overheat, and, at increasingly high temperatures, the zirconium cladding will oxidize and could fail, the fuel pellets will release the fission products from the metallic matrix, and the physical configuration could change. Zirconium oxidation can result from steam at high temperatures. This reaction produces hydrogen, and, being exothermic, the temperature rises faster. Thus, the removal of decay heat is an important safety function.

The other process operation is the removal of radioactive materials, released from the fuel assemblies, that get into the water. These radioactive atoms initially may have been inside the fuel pellet uranium dioxide matrix, then may have diffused out through pellet grain boundaries and escaped into the water from the zirconium tube through minute leak pathways, or the radioactive atoms could have been adhered to the outside of the assembly, due to material impurities in the reactor coolant water, and become irradiated during reactor operation. These radioactive atoms are removed from the fuel pool cooling water by the filtration and ion exchange operations. Figure 2 shows the schematic of these cooling and purification operations.

For the example application of orthogonal factorial analysis, a simplified fault tree was developed. The complete fault tree includes all mechanisms by which the top event could occur. For instance, loss of fuel cooling could be the top event and it would involve loss of water from the pool, loss of ventilation, loss of

physical geometry, etc. In this example, the loss of pool cooling water is shown as the failure mode for the heat removal function. Because of the interconnection of open systems to the closed loop cooling and purification systems, and because of the cross tying of the redundant cooling loop systems by the common purification system, this was anticipated to have the greatest probability for mixup and for interaction. Figure 3 shows the simplified fault tree.

Once the fault tree is constructed, the elements are coded. The failure rates, if known, are then assigned. For this example, the top event is failure of the fuel pool cooling. This is caused by the simultaneous failure of the make-up water supply and the loss of inventory of the closed loop cooling water. Make-up is provided automatically by level controllers from a demineralized water system. In order to simplify the example, the various failures of the addition of make-up water to the balancing tank (i.e., the level control instrument and the automatic block control valve) were considered, but the demineralized water system was considered a single element.

Some of the failure rates were given constant values. (The failure of the demineralized water make-up system was set at 3.72×10^{-6}.) Those components that have a range of failure rates (due to uncertainty, selection of particular component, etc.) are given a variable term. The range for the variable is set in this example from 10^{-3} to 10^{-6} with the average being $10^{-4.5}$.

Five components, designated as X_1, X_2, X_3, X_4, and X_5, were analyzed for their effects on the system availability Q and mutual interactions. For these components, failure rates were varied within the interval 10^{-6} to 10^{-3}. Other components included in the fault tree were assumed to have constant failure rates shown on the tree.

Sixteen computer runs were performed for evaluation of system availability. Conditions for each run were in accordance with the orthogonal matrix shown in Table 1. In this table, values -1 and +1 are used for failure rates 10^{-6} (lower bound) and 10^{-3} (upper bound), respectively, as adopted for standard orthogonal matrices.

The following model for availability Q is developed using expressions (6) and (7) to calculate the coefficients:

$$Q \times 10^{-5} = 8.83 - 8.82\,X_1 - 4.39\,X_2 - 4.39\,X_3 - 0.638\,X_4 - 0.638\,X_5 + 4.38\,X_1X_2 + 4.38\,X_1X_3 + 0.63\,X_1X_4 + 0.639\,X_1X_5 \quad (8)$$

$X_1 \ldots X_5$ = coded failure rates for components X_1 through X_5

The following relationship exists between coded and actual failure rates values:

$$X = \frac{\text{Upper (Lower) Bound} - \chi o}{\Delta\chi} \qquad (9)$$

where:

χo = mid-value between upper and lower failure rates bounds
$\Delta\chi$ = the difference between upper or lower bound and mid-value.

The analysis of this equation shows that the event X_1 has the greatest effect on system availability and X_4 and X_5 have the smallest. This means that components responsible for the event X_1 must be selected carefully. Values X_4 and X_5, by contrast, are allowed to have more uncertainty in failure rate variation, and are probably less costly.

The most significant interactions are between X_1 and X_2, and X_1 and X_3. Failure of any of them will effect the total availability as a common mode failure. Additional redundancy may be recommended in this part of design or more reliable components must be used.

CONCLUSION

The proposed technique, based on a combination of FTA and OFD analysis, can be applied effectively to identify, rank, and evaluate component importance and possible component interactions within the system. The method is expected to be especially useful in comparing alternate system designs and detecting potential weaknesses. In contrast to FTA, only relative failure rates are required for quantitative analysis.

Because the orthogonal matrices allow a high level of standardization, the method is reproducible, flexible, and easy to implement. It also provides a powerful analytical means for:

- Revealing which components contribute most to system availability.
- Comparing the relative importance of single system or component failures.
- Comparing design alternatives for upgrading system availability in a cost-effective manner.

Once constructed for a system, the orthogonal matrix may be applied to different systems and designs, thus providing a high level of standardization and reproducibility.

REFERENCES

1. M. L. Yampolsky and R. O'Mara, Use of Factorial Design for the Analysis of System Interactions in Nuclear Power Plants. Presented at ANS Meeting, October 20-November 3, 1983.

2. S. Addelman, Equal and Proportional Frequency Squares, J. Amer. Statistical Association, 62, 1967, pp. 226-240.

3. M. Leikina (Yampolsky), Mathematical Design of Experiment in Light-Aging of Polyethylene Films, International Chemical Engineering, V. II, No. 2, 1971 (USA).

4. S. Addelman, Symmetrical and Asymmetrical Fractional Factorial Plans, Technometrics, 4, 1 1962, pp. 47-58.

TABLE 1

ORTHOGONAL MATRIX

Computer Run n =	Component Failure Rate				
	X_1	X_2	X_3	X_4	X_5
1	+1	+1	+1	+1	+1
2	+1	+1	+1	-1	-1
3	+1	+1	-1	+1	-1
4	+1	+1	-1	-1	+1
5	+1	-1	+1	+1	-1
6	+1	-1	+1	-1	+1
7	+1	-1	-1	+1	+1
8	+1	-1	-1	-1	-1
9	-1	+1	+1	+1	-1
10	-1	+1	+1	-1	+1
11	-1	+1	-1	+1	+1
12	-1	+1	-1	-1	-1
13	-1	-1	+1	+1	+1
14	-1	-1	+1	-1	-1
15	-1	-1	-1	+1	-1
16	-1	-1	-1	-1	+1

TVO-KPA-VARASTO

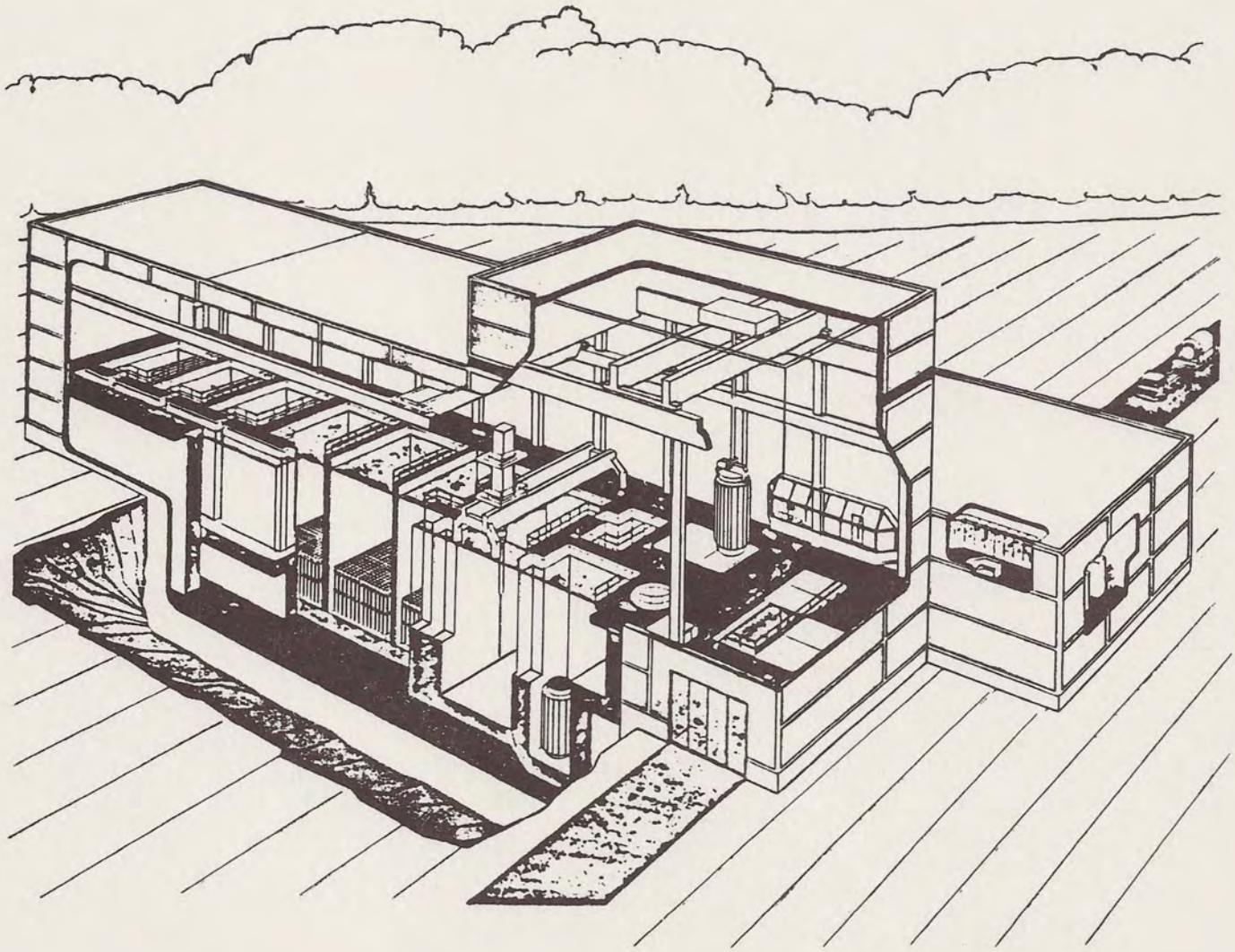

FIGURE 1

STONE & WEBSTER

FUEL POOL COOLING AND PURIFICATION FLOW SCHEMATIC

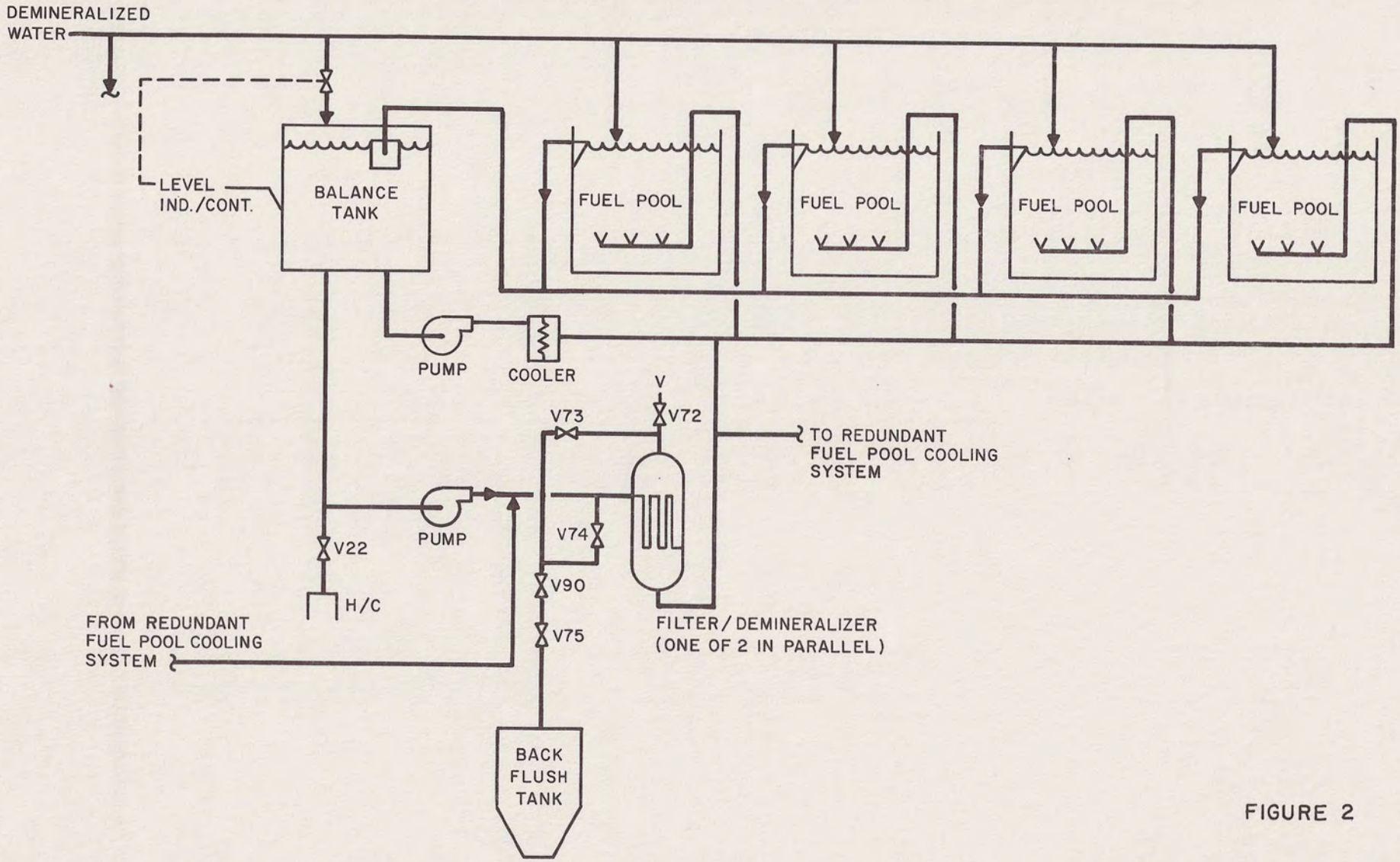

FIGURE 2

STONE & WEBSTER

SIMPLIFIED FUEL POOL COOLING AND PURIFICATION FAULT TREE

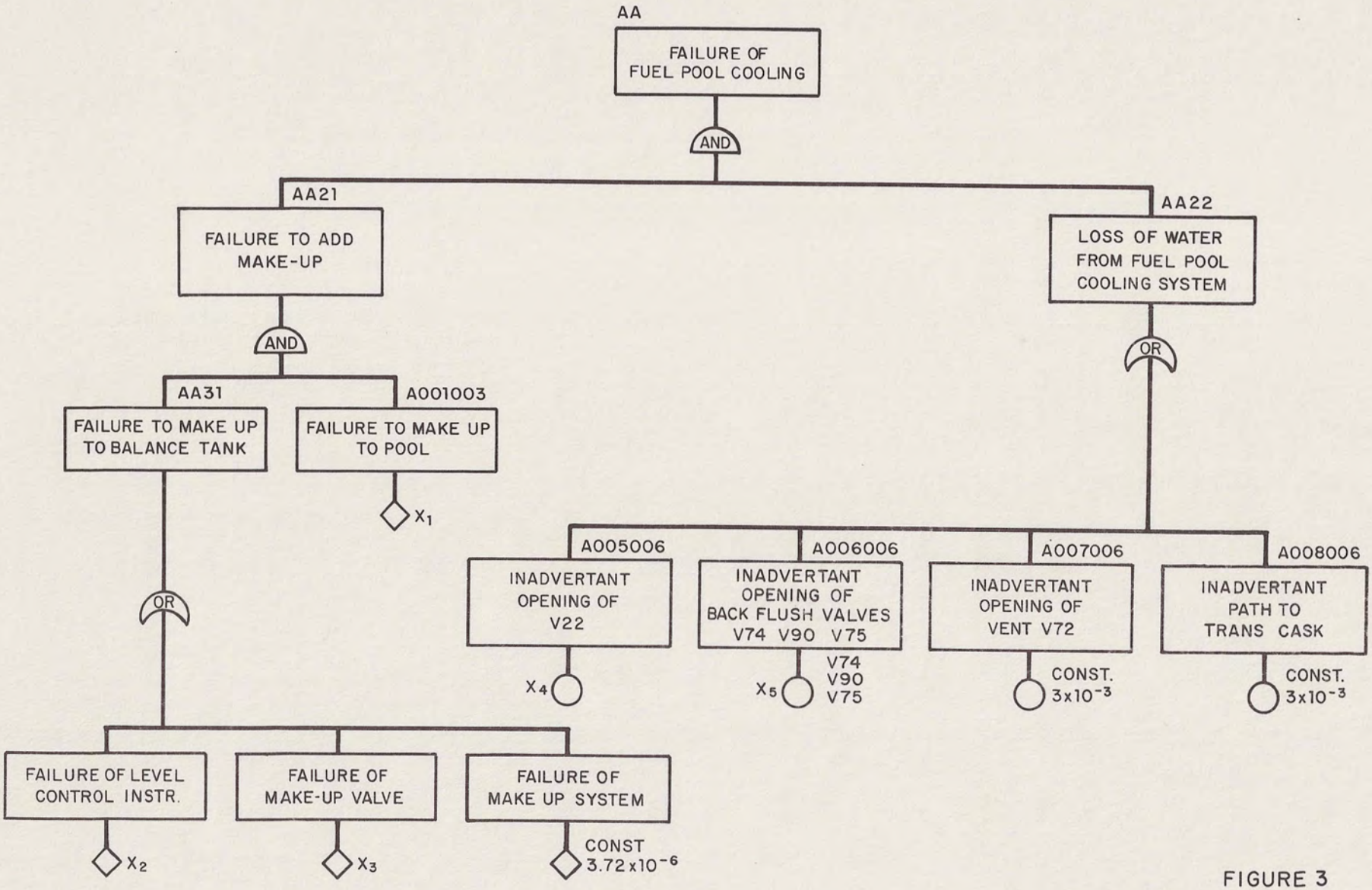

FIGURE 3