Subcontract NP-1

WANL-TME-2502

JUNE 5, 1968

Westinghouse Astronuclear Laboratory

Computer-Programmed Mathematical Model for Reliability

R-109

NERVA NUCLEAR SUBSYSTEM

677555A

MASTER

DRAFT REVIEW COPY

DISCLAIMER

Subcontract NP-1

WANL-TME-2502

JUNE 5, 1968

Westinghouse Astronuclear Laboratory

Computer-Programmed Mathematical Model for Reliability

R-109

NERVA NUCLEAR SUBSYSTEM

677555A

MASTER

DISTRIBUTION OF THIS DOCUMENT UNLIMITED

DRAFT REVIEW COPY

APPROVED BY:

R. F. Dickson
NERVA I Projects Manager

INFORMATION CATEGORY
Unclassified
6/5/68
AUTHORIZED CLASSIFIER DATE

1.0 COMPUTER-PROGRAMMED MATHEMATICAL MODEL FOR RELIABILITY

R109

1.1 INTRODUCTION

The purpose of this report is to describe the work accomplished to date in developing and implementing a computer programmed mathematical model for NSS reliability analysis. The scope of this report is limited to those principal parts of R109 which are consistent with the stage of development of the program. These include:

1) Definition of model requirements.
2) Initial model development.
3) Application of the model to the NSS.
4) Other uses of the computer model.
5) Work remaining.

Definition of computer programmed mathematical model requirements:

1) The model when entered in the computer will enable the reliability to be measured at any level desired. (Component or Subsystem)
2) The model will be compatible with the Reliability data systems described in R108, and capable of utilization in the reporting requirements described in R110. (These data items will be developed later.)
3) The model will be capable of describing all the success (failure) paths that define the mission; i.e., all conceivable series/parallel arrangements of Reliability block diagrams.
4) The model will provide capability for analysis of interactions, and system sensitivity to component reliability.

5) The model will provide the capability for failure-cause analysis.

6) The model be flexible to accommodate changes and/or growth.

2.1 INITIAL MODEL DEVELOPMENT

In the work to date, WANL reliability has adapted an existing generalized computer programmed model, called RVAT (Reliability and Vulnerability Analysis Technique) to the needs of our present program. This mathematical model will meet all the requirements indicated above. In addition, it contains special features which provide the capability for modeling failure-cause events useful in mission reliability studies and failure analysis. A description of the model follows.

2.1.1 Description of the Model

WANL Reliability has developed a generalized mathematical model which provides the capability of computerizing any conceivable reliability block diagram. The model provides a systematic means to combine any configuration of logic <u>and</u> and logic <u>or</u> gates and to compute the reliabilities (or vulnerabilities) for these combinations.

2.1.2 Bases for a Model

The model is based on the development of a Failure Cause Diagram (Fault Tree) for the system to be evaluated. An example of a Failure Cause Diagram (FCD) is given in Figure 1.

In the example the following is apparent:

1) The left branch of any vertical line (or gate) is an effect.

2) The right branches of a vertical line are causes.

3) The diagram proceeds from a (system) level at the left to a detail level (component, material, process) at the right.

This example considers only first order failures. For conditions of two or more failures or timing coincidence for certain events, <u>and</u> gates are used.

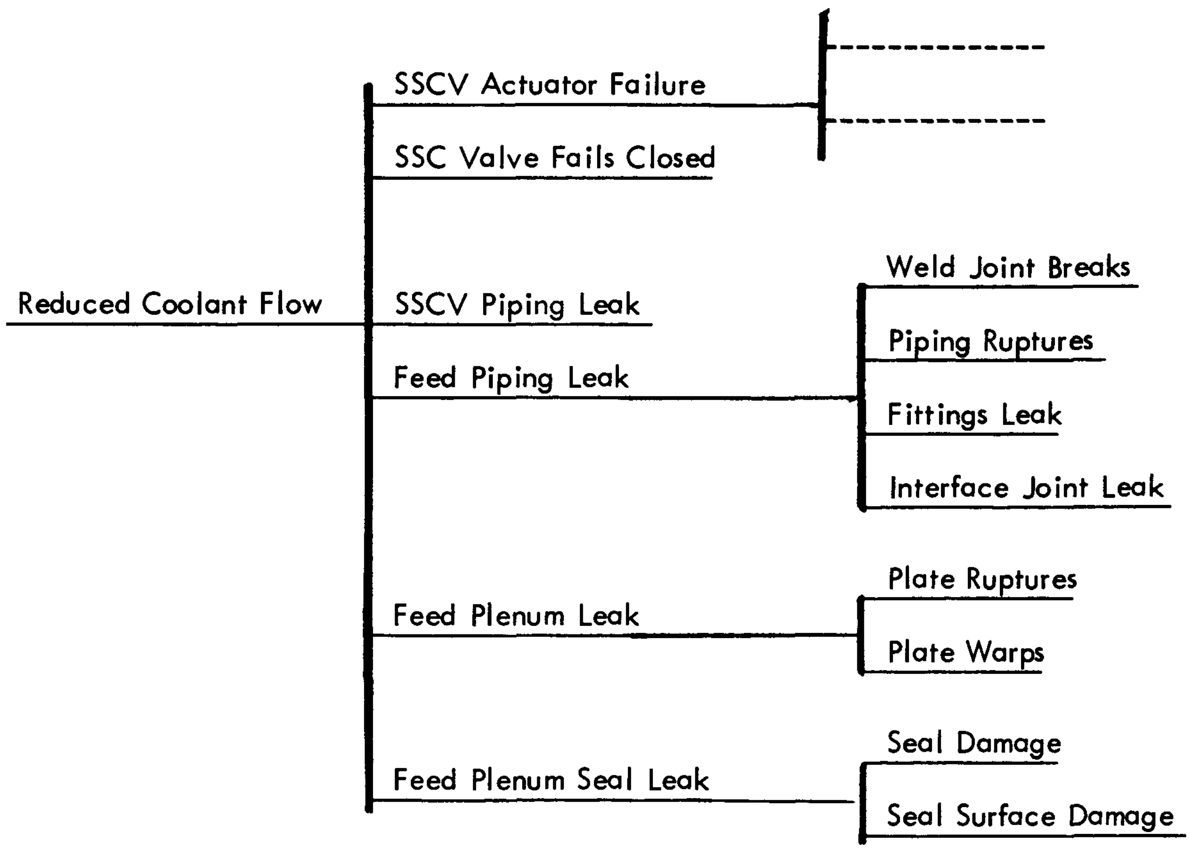

FIGURE 1 Example Failure Cause Diagram

It is likewise clear from Figure 1 that the model will describe all the success (failure) paths for a system such as the NSS. Furthermore, the failure cause diagram uses a symbolic logic (and, or) which is amenable to evaluation by the use of probablistic functions which follow the rules of the logic.

As shown in Figure 2, a Failure Cause Diagram can be visualized as a logical network or "tree" whose apex is a single event, generally the failure mode of a system under study. Unidirectional paths, comprised of branches which connect events at various levels are logically combined to form the "tree." This logic "tree" as described above, forms the basis for the model.

2.1.3 Inserting the Model in the Computer

The detailed description of inserting the model requires some definition of terms. The following definitions apply to the failure cause diagram and its use in the computer model.

1) A level is defined as the number of gates through which the logic has passed. It is obtained by counting gates passed (columns) from the zeroth level. Thus the decade position identifies the logic level.

2) A branch is the logic path at a given level. It is the output of a logic function identified by the branch code. It is the input to the next lower order logic function.

3) A path is the sequence of logic followed through one or more levels to the branch and level of interest.

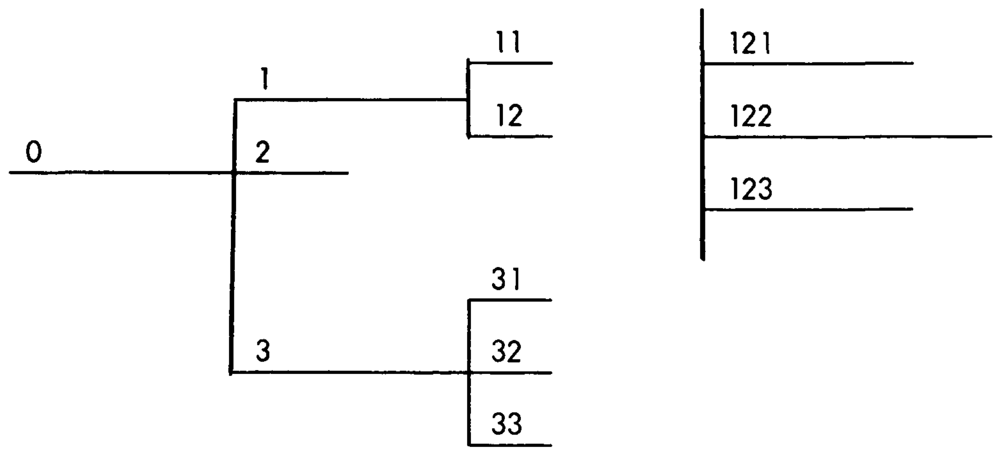

FIGURE 2

Since the FCD is a failure model, we are concerned about failure distributions. The failure distribution at a branch is determined by the failure distribution(s) of all higher level paths which converge on the branch; i.e., if branch 1 for example, then all branches whose first digit is 1 will be considered.

The last branch in any path will have a well defined, independent failure distribution. This principal data must be input to the model. It may be actual data, or assumed data for sensitivity analyses.

The data for the last branch in any path is input in one of the following ways:

1) Value is read from the branch input card, i.e, the failure probability number.

2) Value is computed for the function $1 - e^{-\lambda t}$ where t is read from the branch input card and λ is read in at the beginning of execution.

3) Value is computed for the cumulative normalized distribution $1/2 \ (1 + \text{erf} \ (\frac{x - u}{\sqrt{2}\sigma}) \ )$ where x is read from the branch input card and u and σ are read in at the beginning of execution.

4) Value is computed by linear interpolation (val $= y_1 + (\frac{y_2 - y_1) (x - x_1)}{x_2 - x_1}$

where x is read from the branch input card and x_1, x_2, y_1 and y_2 are found from a table which was read in at the beginning of execution.

The following rule is used to determine the failure distribution at a branch where "or" logic is used.

$$Q_x = 1 - (1 - Q_{10x+1}) (1 - Q_{10x+2}) \ldots (1 - Q_{10x+K})$$

where x is the branch in question, and there are as many as k branches of a higher level which are "or" inputs to the logic for branch x.

The following rule is used to determine the failure distribution at a branch where "and" logic is used.

$$Q_r = (Q_{10r+1}) (Q_{10r+2}) \ldots (Q_{10r+s})$$

where r is the branch in question and there are as many s branches of a higher level which are "and" inputs to the logic branch r.

It is evident that this model is directional and that the highest level distributions must be determined first. Then, proceeding back through the branches along the logic path, the failure distribution at the zeroth level (or at any branch) may be determined.

2.1.4 Operating the Model - Steady State

The steady state failure distributions introduced into the model are sampled via criteria determined by the input parameters. This input state for the model results in a discrete output state for each branch by applying the rules noted above. A record of all branch values at this time provides a map of critical paths for the model. The sensitivity of the model to particular paths may be investigated by altering distributions (one or more) and re-evaluating.

2.1.5 Output

The probability for each branch will be printed along with the branch number and the description of the branch.

A separate output page will be printed for the branch which has the most critical effect on the system.

3.1 APPLICATION OF THE MODEL TO THE NSS

There are two principal areas of application for the generalized model described above. The first is the application of an appropriate model for assessing reliability which is keyed to the configuration of CEI's and ECC's and their respective components. The second is the application of event oriented failure cause studies, such as mission reliability studies which will be discussed in section 4.1, below.

In applying the model for reliability assessment of the NSS, the FCD was developed on the basis of the reliability block diagram used for allocation as shown in Figure 5 and as described in R103. The step from the reliability block diagram to the Failure Cause Diagram for the NSS (Figure 3) is straight-forward. To this date, the model has been constructed to the ECC level as shown in Figure 5. The model was tested by assuming that the allocated goals were the first assessment, and inputting these values into the computer model. A sample output from the computer model is shown in Figure 4.

4.1 OTHER USES OF THE COMPUTER MODEL

The flexibility of the generalized mathematical model permits its use in the important area of failure modes analysis. The reliability program dictates a need for failure modes, and effects analyses. When performing a system failure mode analysis for example, undesirable system events are identified, and their causes are traced back through the system to identify the set of primary causes. For each primary cause, the likelihood of occurrence is evaluated in conjunction with determining means to obviate the effect or remove the mode of failure. A systematic approach to an evaluation of this type leads directly to the use of a failure-cause diagram. This diagram may be inserted in the computer as an "event" model. Consider the undesirable event (malfunction, failure) of loss of thrust, for example. A preliminary FCD for this event is given in Figure 6. In this FCD the first order failures have been identified. The probability of the event occurring is obtained by working the model, using a appropriate input failure distribution for the components in question.

It is anticipated that a set of "event" models will be developed for evaluation of mission reliability and ground test reliability. These will provide a principal basis for malfunction studies on system facsimile models.

In addition to the event models application discussed above, it is a reliability requirement that comprehensive failure analysis be made of all system and component failures. It is planned to implement a systematic approach to failure analysis based on the use of the Failure Cause Diagram. Where appropriate, the computerized model of the overall NSS will be used, to determine critical paths for the failure mode in question.

5.1 WORK REMAINING

The computer programmed mathematical model is basically complete in the areas of what is to be done and how it can be done. The final model for assessment, however, depends on a complete definition of the NSS to the level of detail in components (and properties) that is necessary and workable. It is expected that the model will continue to expand from its present ECC level to the detailed part level commensurate with detail design releases, essentially reflecting a current description of the system.

In addition to the growth noted above, a strong communications link between the assessment model, failure cause models and system facsimile models will be developed to assure integration of reliability and other systems evaluations.

The development of the computer programmed Reliability Model will reflect (particularly at the input end) the interraction with data system, failure reporting and status reporting as described in R108, R110.

Finally, the model developed is based on Fortran IV programming, and it is planned to coordinate with the prime contractor prior to PDR to assure that no communication problems exist where reliability models interface.

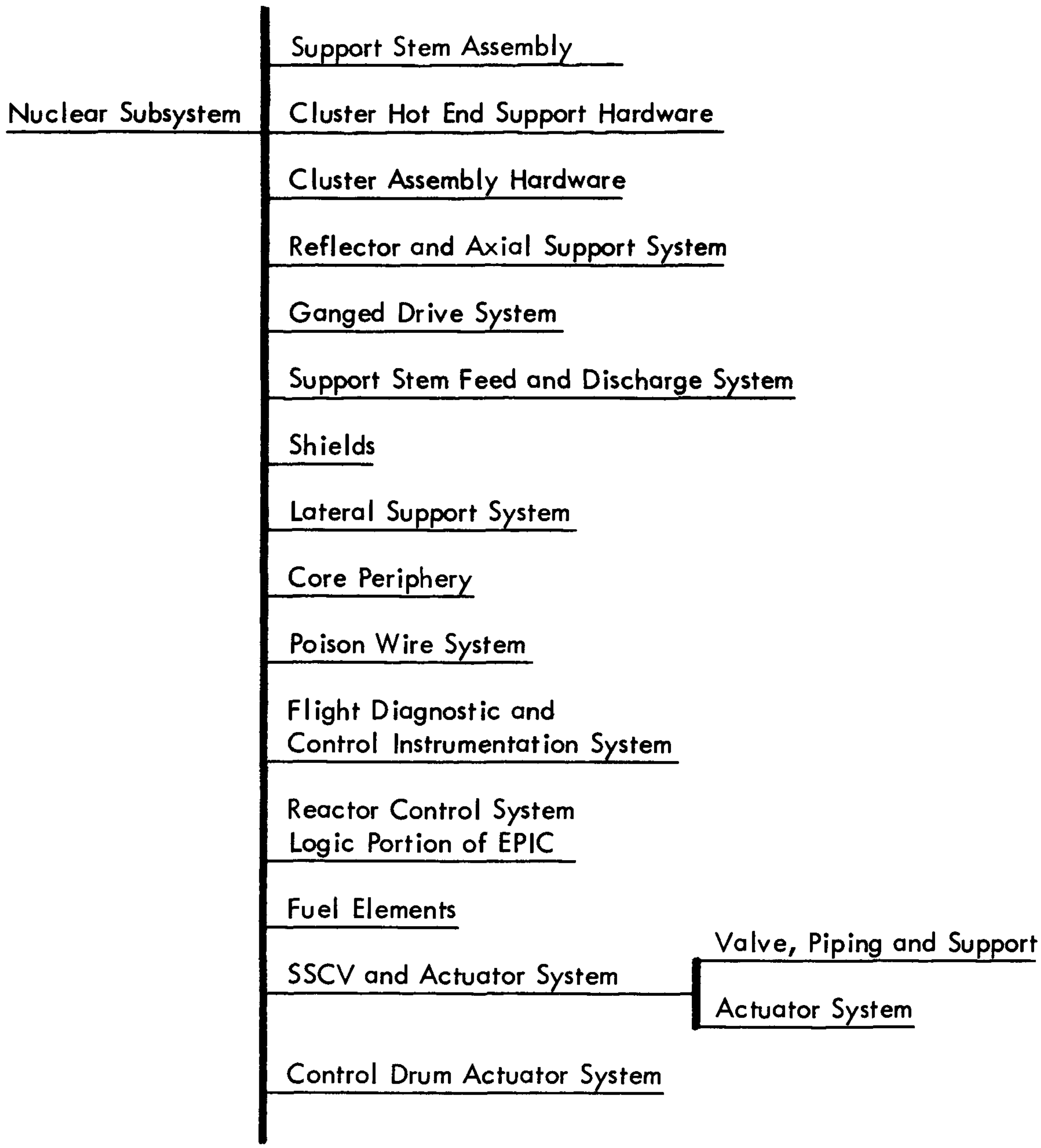

FIGURE 3 NSS Failure Cause Diagram Depicting the Reliability Block Diagram

BRANCH NUMBER	RELIABILITY GOAL Q = 1 - R	COMPONENT DESCRIPTION
0	.0049906096	NERVA ENG
1	.0029966028	WANL
11	.0023682521	GW BRANCH
111	.0001000000	SUPRT STEM ASS ENGRG CRIT COMP
112	.0001100000	CLUSTR HOT END SUPRT HRDWRE
113	.0001000000	CLUSTR ASS HRDWRE
114	.0002900000	REFLECTOR & AXIAL SUPRT SYS
115	.0000400000	SHIELDS
116	.0000400000	LAT SUPRT SYS
117	.0003100000	CORE PERIPHERY
118	.0013800000	FUEL ELEMNTS
12	.0003199606	LS BRANCH
121	.0000600000	CONTRL DRM ACTAR SYS
122	.0000800000	SSCV & ACTUATR SYS
1221	.0000300000	VLUE PIPG & SUPRT
1222	.0000500000	ACTUAR SYS
125	.0000900000	GNGD DRVE SYS
126	.0000100000	SUPRT STM FD DSCHVG SYS ECC
13	.0003099809	JM BRANCH
131	.0000100000	FLT DIAG & CONTR INST ECC SPEC
132	.0000700000	REACT CONTR SYS LOGIC EPIC ECC
133	.0002300000	POISON WIRE SYS ECC
2	.0020000000	AEROJET

FIGURE 4 NSS Computerized Reliability Model (Typical Output)

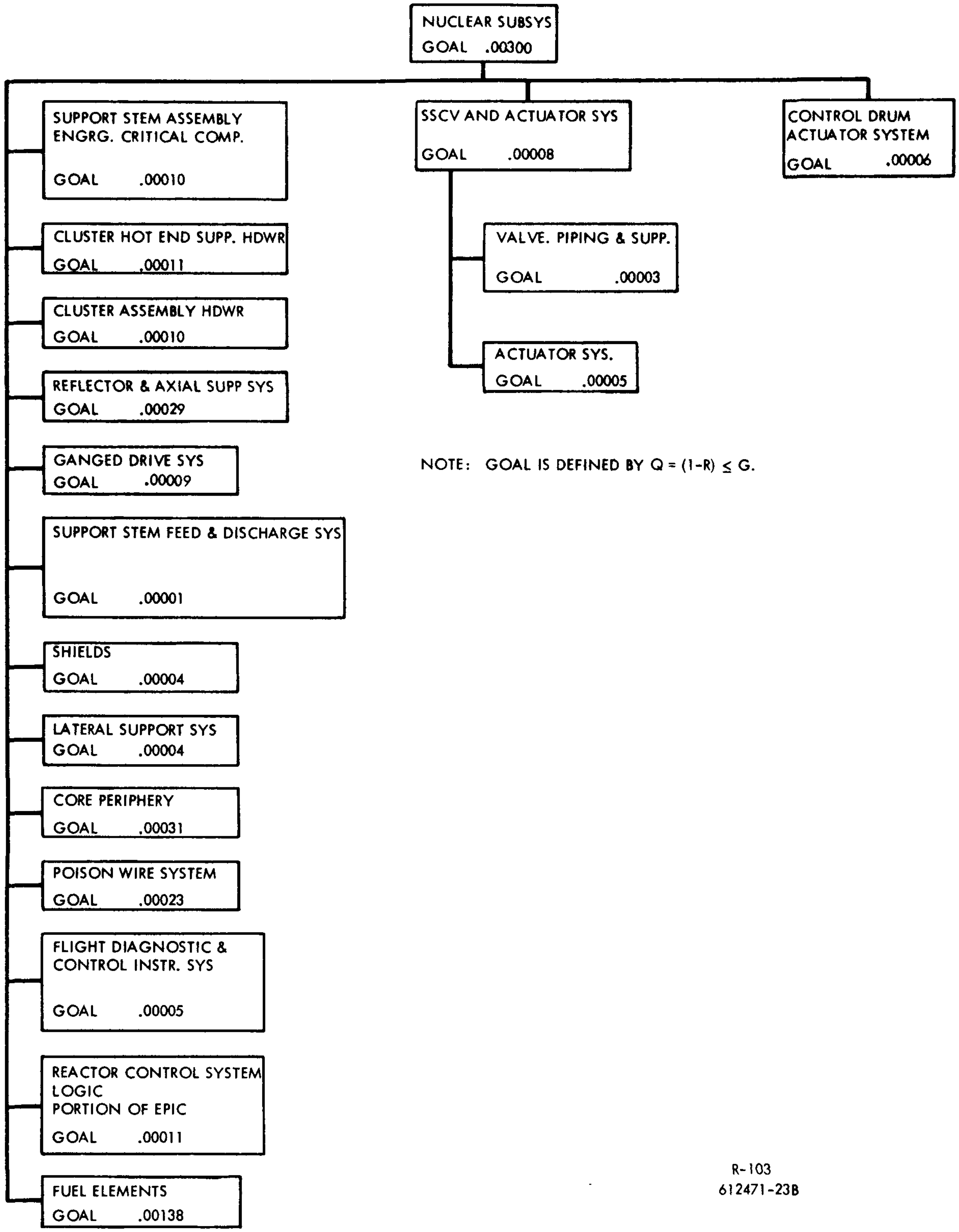

Figure 5. Reliability Block Diagram of the NSS to the ECC Level

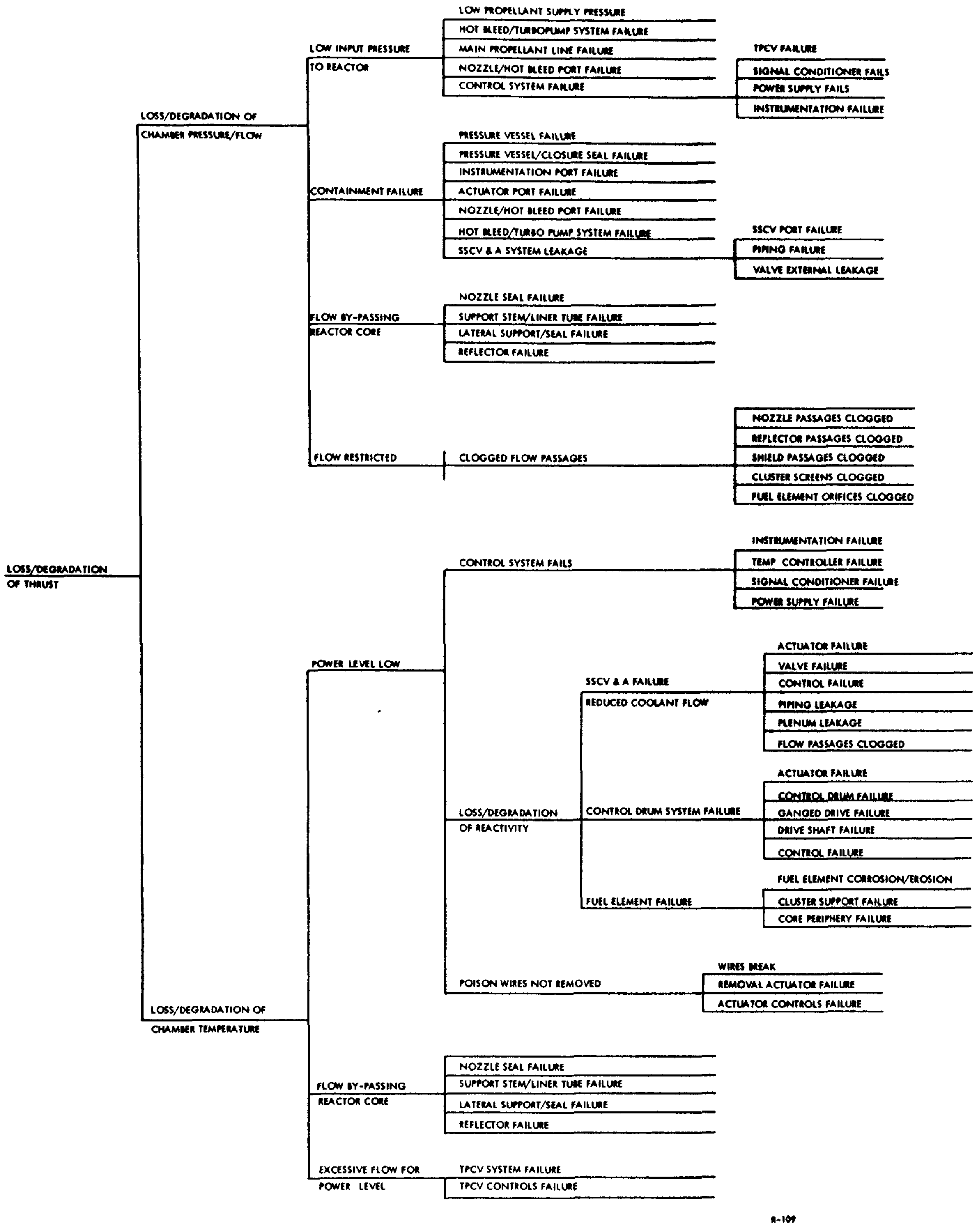

Figure 6. Preliminary Failure Cause Diagram for Loss/Degradation of Thrust