RECEIVED BY OSTI APR 29 1985

CONF-8504126--1
CONF-850610--28

MASTER

CONF-8504126--1

DE85 010487

Ultra-Reliable Computer Systems - An Integrated Approach for Application in Reactor Safety Systems

by

G.H. Chisholm

EBR-II Division
Argonne National Laboratory
P.O. Box 2528
Idaho Falls, Idaho 83403-2528

The submitted manuscript has been authored by a contractor of the U. S. Government under contract No. W-31-109-ENG-38. Accordingly, the U. S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for U. S. Government purposes.

Submitted for Presentation
at the
EPRI Fault-Tolerant Systems Seminar
April 1985
Phoenix, Arizona
and Presented/Published
at the
1985 ANS Summer Meeting
June Boston, Mass.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

Section 1

INTRODUCTION

Improvements in operation and maintenance of nuclear reactors can be realized with the application of computers in the reactor control systems. Table 1 is a partial liting of potential beneficial uses. In the context of this paper a reactor control system encompasses the control aspects of the Reactor Safety System (RSS). Equipment qualification for application in reactor safety systems requires a rigorous demonstration of reliability. For the purpose of this paper, the reliability demonstration will be divided into two categories. These categories are demonstrations of compliance with respect to a) environmental and b) functional design constraints. This paper presents an approach for the determination of computer-based RSS respective to functional design constraints only. It is herein postulated that the design for compliance with environmental design constraints is a reasonably definitive problem and within the realm of available technology. The demonstration of compliance with design constaints respective to functionality, as described herein, is an extension of available technology and requires development.

Table 1

Reactor Control System Enhancements*

1. Improve plant availability via appliation of advanced control and observation techniques.
2. Backfit of computer based systems in place of complex analog systems where multiplexing saves significant installation dollars.
3. New designs, especially space reactors, where automatic operation is a necessity.
4. Improve control system flexibility to implement changes (both backfit and new).

* Enhancement provided through the application of computers versus traditional analog control.

Section 2

USE OF COMPUTERS IN REACTOR SAFETY SYSTEMS

Background information pertaining to the regulatory environment and specifically to the application of computers to reactor safety systems is provided through a description of a current project involving Experimental Breeder Reactor II (EBR-II). The Full Authority Fault-tolerant Reactor Control System (FAFTRCS) being developed at Argonne National Laboratory encompasses this design philosophy and safety strategy.

Because the FAFTRCS project is dependent upon developing technologies, the 5-to-7 year effort has been subdivided into three phases. The earlier phases are intended to demonstrate evolving technologies in support of the next phase.

Phase 1, Fault-tolerant Flow Trip (FT^2), is focusing on V&V of the generic issues for ultra-reliable computer-based control, i.e., fault-tolerant processor, developing automated aids for V&V, and application of signal validation software. Phase 1 will culminate with the installation of a fault-tolerant flow channel in the EBR-II PPS.

Phase 2, Fault-tolerant Analytical Redundancy, will expand the software V&V methods developed during phase 1. In addition, multi-variable models will be validated for reactor control. Phase 2 will culminate with a demonstration of V&V techniques for medium software packages plus a demonstration installed at EBR-II.

Phase 3, FAFTRCS, extends analytical redundancy techniques into the realm of total control.

Systems that are designed for reactor protection must adhere to stringent design requirements to ensure reliable protection. Because of the complexity of computer-based system, an adequate reliability demonstration becomes a vital aspect of this advanced application.

Experimental Breeder Reactor II is a DOE-owned and ANL operated reactor. In accordance with DOE guidelines, a PPS is provided to ensure safe reactor shutdown or to mitigate the consequences of postulated accidents. The PPS is designed in accordance with DOE standard RDT C-16-1T. The intent of this standard is to provide guidance during the design and analysis of the PPS to ensure adequate system reliability.

The general criteria for designing systems important to safety that are invoked for commercial nuclear reactors are codified in Title 10 of the Code of Federal Regulations, Chapter 50 (10 CFR 50) - Appendix A, "General Design Criteria for Nuclear Power Plants." These criteria are further amplified in Regulatory Guides which are published by the Nuclear Regulatory Commission and which comprise regulatory endorsement for standards published by various technical organizations, including the Institute of Electrical and Electronic Engineers (IEEE) and the American Nuclear Society (ANS). The desire for inclusion of computers into reactor safety systems has propagated a joint ANS/IEEE standard. [See Ref. (1).]

Recently the designer of safety systems for DOE reactors has had to become cognizant of both sets of standards and ensure that the final design complied with their intent. [See Ref. (2).] Specifically, the intent of the FAFTRCS project is to demonstrate a methodology for design verification of computer-based reactor-safety systems that complies with these standards. The need for such a demonstration is exemplified in Ref. (3), which identifies the number of Licensee Event Reports which are traceable to design errors in the application of plant computers at operating nuclear plants. This report highlights the difficulty that designers and regulators are experiencing in applying computers to reactor shutdown systems (RSSs). The difficulty arises from the complex nature of computer-based systems and of reliability analyses for the design. Analysis of reactor safety systems requires detailed qualitative and quantitative examination of the design, e.g., fault-trees, failure modes and effects, Markhov, etc. The complex nature of computer-based systems increases the manpower requirements for similar analyses.

A form of software analysis which could be considered analogous to that required for RSSs is a formal proof of correctness (POC). A formal POC is an extremely rigorous proof of the properties of the software and claims to be entirely exhaustive in approach. There are two methods of performing a formal POC:

(1) an analytical process or (2) testing. The analytical process suffers the limitation that its execution is dependent upon the analyst and is therefore subject to human error. The testing process involves duplicating every error (both software and hardware induced) for every execution path. This type of testing may take tens of thousands of hours to perform and is also subject to human frailities. Reference (4) outlines a practical approach that combines both testing and POC. The underlying theory is that both processes are incomplete, but that a testing program based upon confirmation of the assumptions and assertions inherent in the POC would provide validation of the analytical POC without the manpower burden inherent in a test-based POC. This theory will form the basis of design verification for the software and hardware components of the fault-tolerant flow-trip demonstration.

Table 2 identifies additional problems which will be addressed during the FT^2 phase. The formal analysis and testing described in the preceding paragraph are theoretical until validated; therefore, there must be a method for providing this validation. One method for determining reliability and therefore validating these techniques is software reliability modeling. References (5) and (6) describe a number of techniques for software-reliability modeling. Applying the best available approach to the software design would be an additional form of validation.

Table 2. Fault-tolerant Flow-trip Problems and Proposed Solutions

Problem	Proposed Solution
Software reliability	Formal analysis validation via testing reliability modeling
Model certification	Testing in actual environment analysis via dynamic simulation of nuclear plants (DSNP) code
Hardware reliability	Ancillary equipment - traditional computer - fault-tolerant properties confirmed via formal analysis and validation testing
System validation	Testing in two phases: (1) bench tests to validate design, and (2) in-plant tests to provide acceptance.

The availability of fault-tolerant computers (FTCs) may resolve part of the complexity issue associated with computers, in that the designer can ignore the hardware-related faults. This assumes that adequate failure detection and identification features are incorporated to correct identifiable faults, and that analysis supports sufficiently long periods of operation between diagnostic tests.

The words "fault-tolerant computer" connote different things to different people. To a system operator for a financial institution the words mean that the transaction will be processed without fault. The machine that accomplishes this processing may rely on techniques which are unacceptable for real-time applications, but which perform as required for the transaction environment. However, the words "fault-tolerant" connotes the capability of being universally tolerant of faults. This implies the totality of faults, including those residing in software. The software fault is the most insidious of faults as it does not have the predictable nature associated with hardware faults. Software in the context of a reactor control system must be considered a unique entity in contrast to the un-uniqueness of analog, i.e., there are millions of installations of identical analog components but relatively few for software. This disallows any credit for failure predictions and belies the terminology "fault-tolerance," i.e., the myth of fault-tolerance is that the fault-tolerant nature of the machine is easily defeated by the application software.

The hardware component of the design-verification problem has two parts. The first part is associated with the fault-tolerant properties of the computer. To take credit for the benign nature of the effect of the hardware upon the formally analyzed software, the design must use fault-tolerant hardware. That is, the hardware must be configured so that it will not introduce failures into the software job stream. Fault tolerance within this context, means that no single fault will introduce a software failure. However, for the design to be able to take credit for fault-tolerance, those properties of the design which produce fault tolerance must be formally verified. This verification will take the form of formal analysis of the design for properties essential to fault tolerance and validation of the design via testing.

The techniques for accomplishing the task of design verification and POC at ANL utilize an automated-reasoning program developed by the ANL Mathematics and Computer Science Division. The technology requires further development to

accomplish the tasks defined for the fault-tolerant flow trip, and the project is dependent upon this further development to attain complete success within a reasonable time. However, a further development in formal analysis will benefit the design process, even if rigorous POC is not forthcoming.

Progress to date includes a modeling technique that is amendable to hardware and software representation as well as their interaction. This modeling technique is also heirarchical by nature and has been structured to support the safety review aspect for potential liscensing. Further definition of the modeling methods will be the subject of future publications.

The underlying assumption of formal analysis is that the model of the plant is an accurate representation of the plant. This project will use two techniques to certify the accuracy of the model. The first will use a whole-plant modeling program developed under the Dynamic Simulation of Nuclear Plants (DSNP) code. This method will allow parametric analysis of the flow model with respect to plant upsets. The second method will be to install the model in a test environment where it will use actual plant signals, and the test will duplicate the final installation. The test will be monitored to verify accurate flow-trip response.

A final attribute of the safety argument being proposed for acceptance of the fault-tolerant flow trip project is that of determination of the safety boundary both in the hardware and software environments. The design of the software for the recommended design is dependent upon the operation of a sequential probability ratio test (SPRT). The SPRT is a statistically based test of sensor information, which incorporates the predicted failure distribution of the sensor. The output of the SPRT is one of three hypotheses: (1) the sensor is correct, (2) the sensor is incorrect, or (3) additional data must be gathered. The intent is that the SPRT be the heart of the flow trip, i.e., the SPRT is the functional element of the design that must perform infallibly. The SPRT in this design might be considered as the counterpart of a coincidence circuit in analog-safety-system designs. The software and hardware necessary for infallible operation of the SPRT must be demonstrated to be reliable and must therefore be subjected to the formal analysis described above. Because the analytical technology is still under development, the amount of software and hardware that must be analyzed has been kept to a minimum for this demonstration.

As mentioned above, the techniques being developed during this project must be validated to provide a useful demonstration. The intent is that a test program will be developed by a separate group of engineers at another contractor. This group will take the design specification and develop a test procedure without significant influence by the design team. (However, there must be some interaction between the test team and the analysis team because of the need for the test to validate the assumptions and assertions made during the analysis.)

The primary aim of this phase of the FAFTRCS project is to demonstrate the acceptability of computers for application in reactor safety systems. Acceptability implies high reliability and availability, and this project intends to demonstrate a design V&V approach which is superior to the V&V that resulted in the incidents reported in Ref. (3).

Section 3

SYSTEM DESIGN DESCRIPTION

Figure 1 is a simplified schematic of the EBR-II Reactor Protection System (RPS). (RPS and Plant Protection System (PPS) are synonomous in this document.) The EBR-II RPS consists of redundant strings of diverse trip signals. The underlying strategy for protection of EBR-II is that the power-to-flow ratio be maintained at or below a predetermined level. The Flow Protection System comprises a subset of RPS as shown on Fig. 2. Figure 3 depicts a subcircuit diagram for a typical flow trip element. Note that a single sensed parameter provides a trip signal for both shutdown string "A" and "B." It is the intent of Phase 1 to duplicate the function of any one flow channel. The intent of Phase 2 is to replace the flow protection system with a combination of analytically derived signals plus direct sensing signals.

The system must be capable of detecting the following types of failures:

(a) Loss or reduction of primary flow
(b) Loss of a sensor
(c) Any single, sequental failure within the FTP

Those components of the system which are essential to detecting these failures will be subjected to formal analysis techniques as well as quantitative reliability analysis to assure conformance to the design requirements.

The following description discusses the design from three standpoints: (a) functional, (b) software and (c) hardware.

Funtional Description

Figure 4 is a functional block diagram of the sytem concept. There are two primary pumps which will provide parametrical information. These signals will be validated by a statistical test. The validated signals are then used to

determine the flow via a pump model. A software vote is taken for the results of flow determination and the voted output is redundantly transmitted to the plant.

Software Description

The application software will be developed in a high-level language on a development system. In conformance with the operating system software, the "C" language will be used. The development system will be capable of in-circuit emulation within the fault-tolerant computer (FTC). Once the software is complete it will be burned into read-only-memory chips.

Figure 5 is a three-level software flow chart for the conceptual design. The functions ascribed to the software include I/O drivers, SPRT, broadcast (which implies synchronization), and voting. This is the minimum capability demanded of the software. The flow chart indicates some of the features of the FTP that require understanding. To maintain the redundant capability of the sensors, each signal is brought into the FTP via redundant plant data interfaces. The next step is to broadcast the exact information that processor A received to the other two processors. The broadcast is accomplished via the interstage registers connected to each processsor's I/O bus. The interstage registers are interconnected by a separate bus devoted to broadcast and synchronization tasks. The interstage registers consist of a number of registers and voting hardware. All reading and writing to and from the processors must be processed through the interstage registers and synchronization is effected by this requirement. When a processor executes a read/write it enters a wait state until the information is available to/from all processors. Normal execution then continues until the next I/O instruction is executed. System software is necessary to support these exchanges and will be within the safety boundary.

Hardware Description (Figure 6)

Sensors for each pump are required as follows:

- Three current sensors
- Three rpm sensors

Peripheral controllers for the FTP will consist of:

- Asynchronous communications controller (may connect to interface)
- Standard bus interface and multiplexer/analog-to-digital converter

FTP hardware will consist of:

- Quadruple Motorola 68000 microprocessors boards
- A highly synchronized backplane bus
- Quadruple interstage register boards (which include the fault-tolerant clock hardware)

Section 4

CONCLUSION

The FAFTRCS project at ANL encompasses the following:

1. Fault-tolerant Computers
2. Automated Methods for Formal Verification of TOTAL Systems via Automated Reasoning
3. Generic Signal Validation Software, and
4. Computer-based Reactor Safety Systems.

Progress to date includes: 1) development of theoretical basis for signal validation, 2) specification of fault-tolerant processor, 3) plant modifications to support experimentation, 4) development of software/hardware model for representation to automated reasoning program, and 5) design of special purpose interface hardware.

Section 5

REFERENCES

1. "Application Criteria for Programmable Digital Computer Systems of Nuclear Power Generating Stations," IEEE/ANS-7.4.3.2-1982.

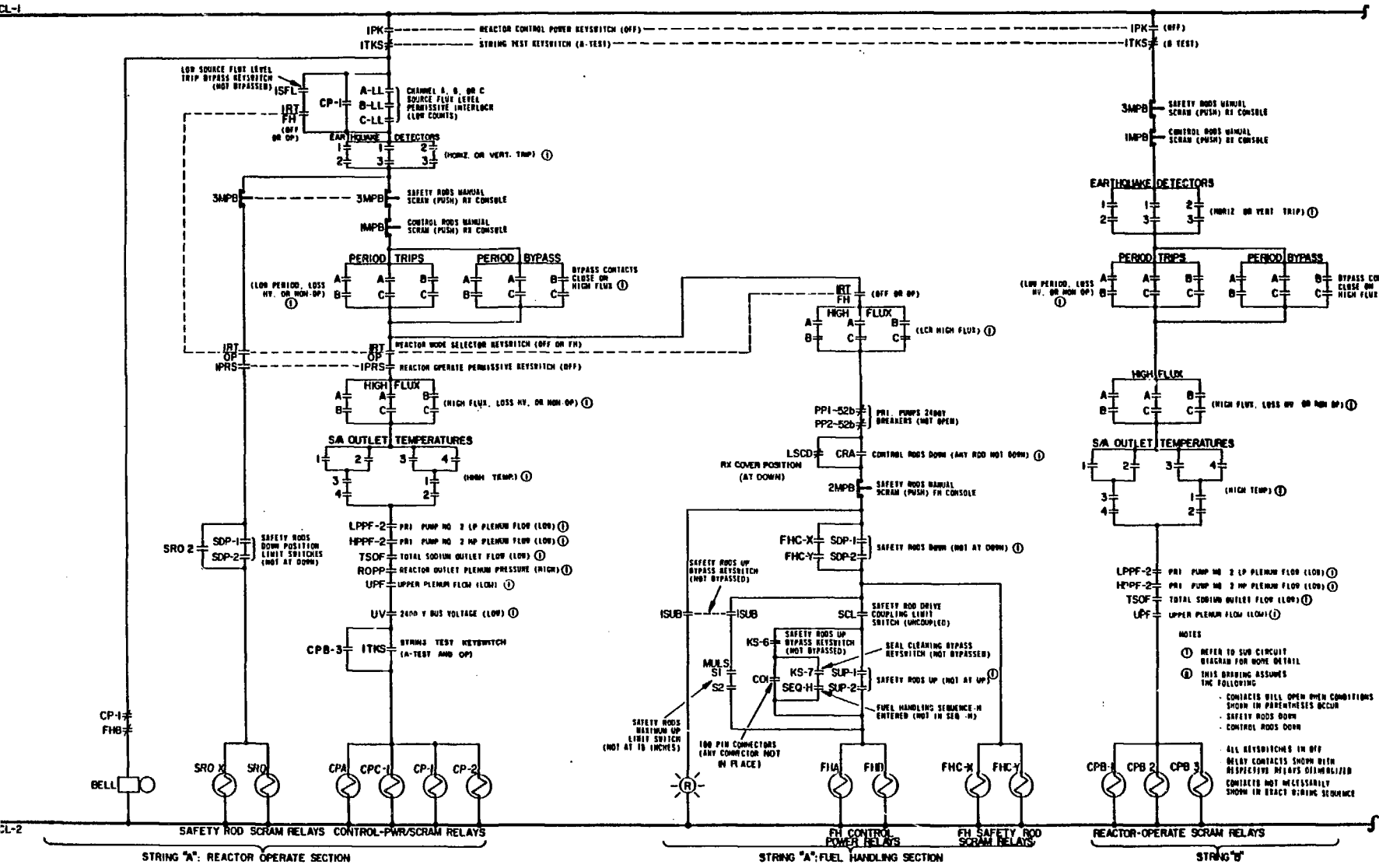
2. "SAREF/TREAT Upgrade Project - Final Safety Analysis Report," Argonne National Laboratory S39942-0001-YT-OA, dated June 1983.

3. R. R. Rohrdanz, "Signal Isolation Device and Stored Program Digital Computer Problems Experienced by U.S. Commercial Nuclear Power Plants," EG&G Idaho EGG-EE-6052, September 1982.

4. J. B. Goodenough and S. L. Gerhart, "Toward a Theory of Testing: Data Selection Criteria," Current Trends in Programming Methodology, Vol 2, pp 44, 1977.

5. J. C. Dekert, et al, "Reliable Dual-Redundant Sensor Failure Detection and Identification for the NASA F-8 DFBW Aircraft," The Charles Stark Draper Laboratory, Inc., May 1977, R1077.

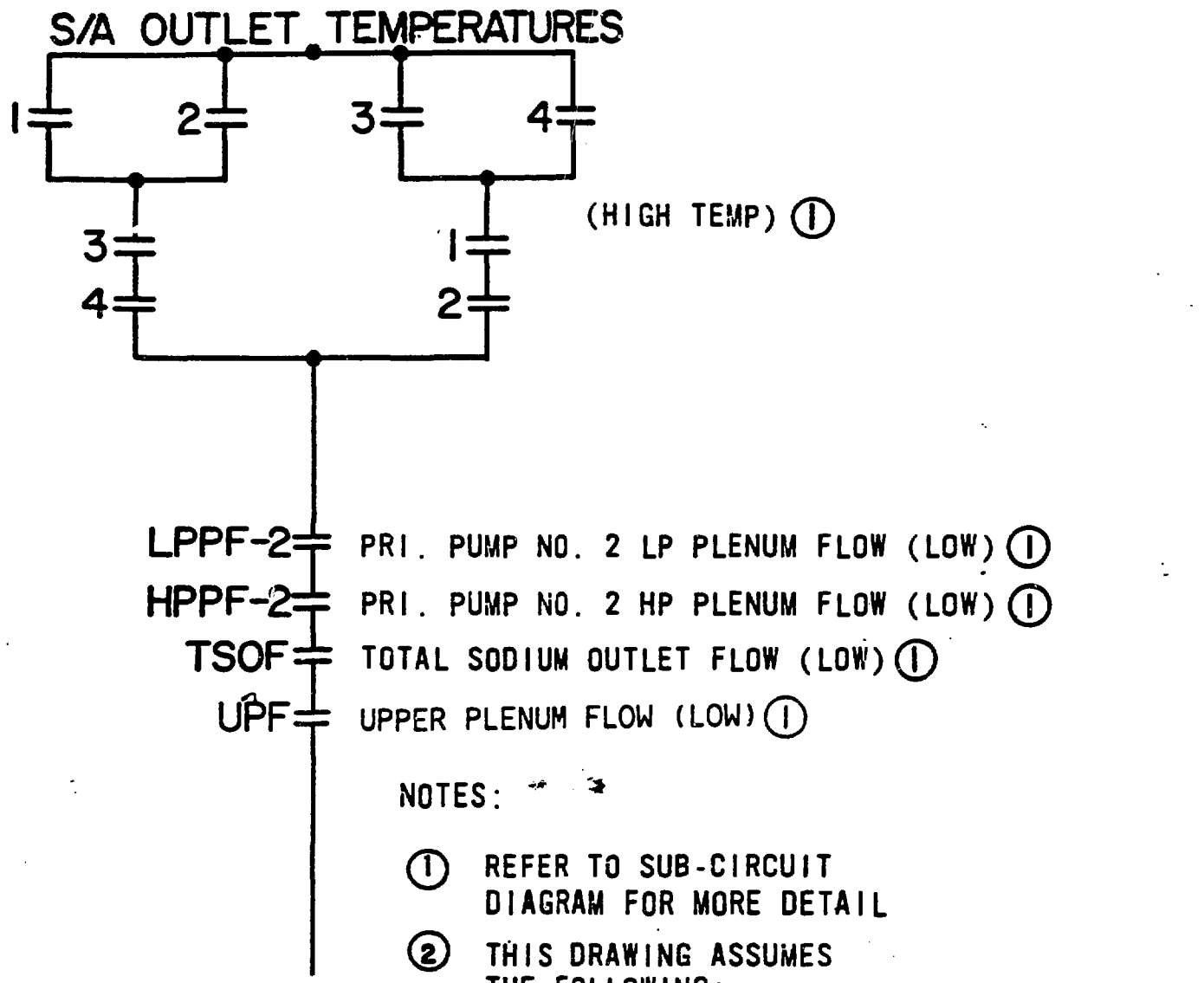
Figure 1



REACTOR SHUTDOWN SYSTEM (RSS) SIMPLIFIED SCHEMATIC

T/P-R-20003-D
REV. 13 6/83

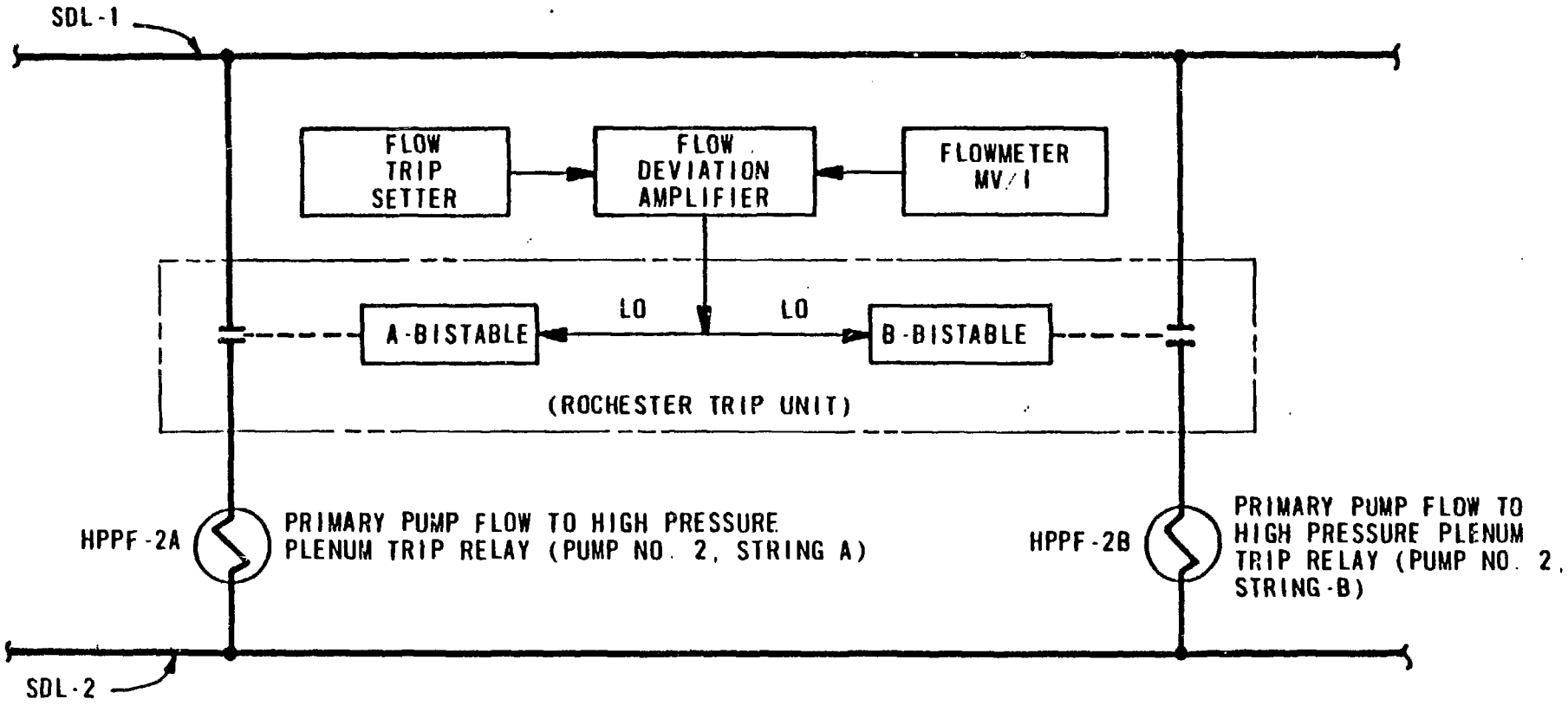
Figure 2



NOTES:

1. REFER TO SUB-CIRCUIT DIAGRAM FOR MORE DETAIL
2. THIS DRAWING ASSUMES THE FOLLOWING:
   - CONTACTS WILL OPEN WHEN CONDITIONS SHOWN IN PARENTHESES OCCUR
   - SAFETY RODS DOWN
   - CONTROL RODS DOWN

Figure 3

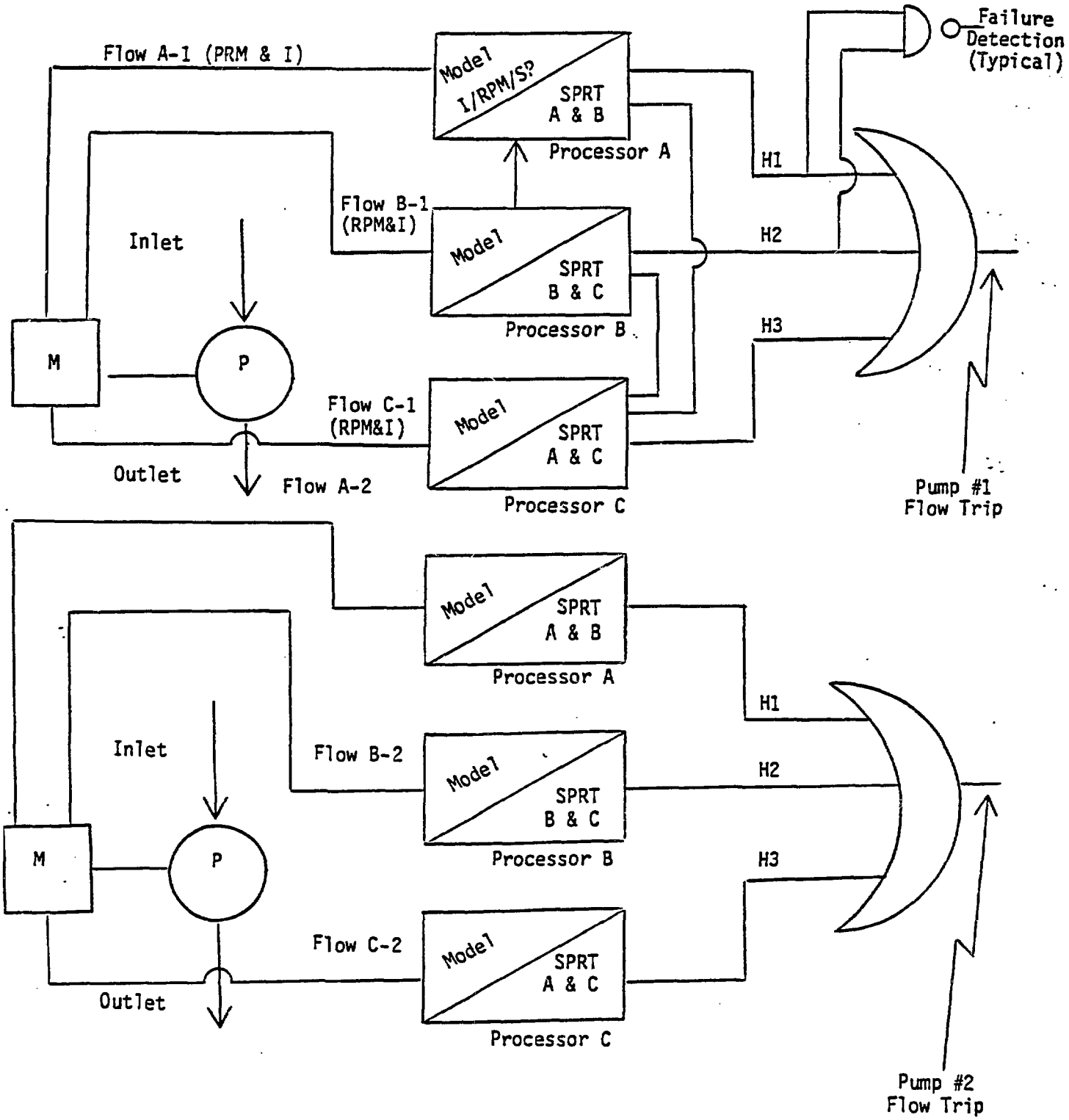


T/P-R-20015-C

PRIMARY PUMP NO. 2 FLOW TO HIGH PRESSURE PLENUM TRIP CIRCUITS FOR SHUTDOWN STRINGS A & B

FIGURE 4

Symmetry "B"



Symmetry - Functional Diagram

FIGURE 5

Symmetry "B" Software

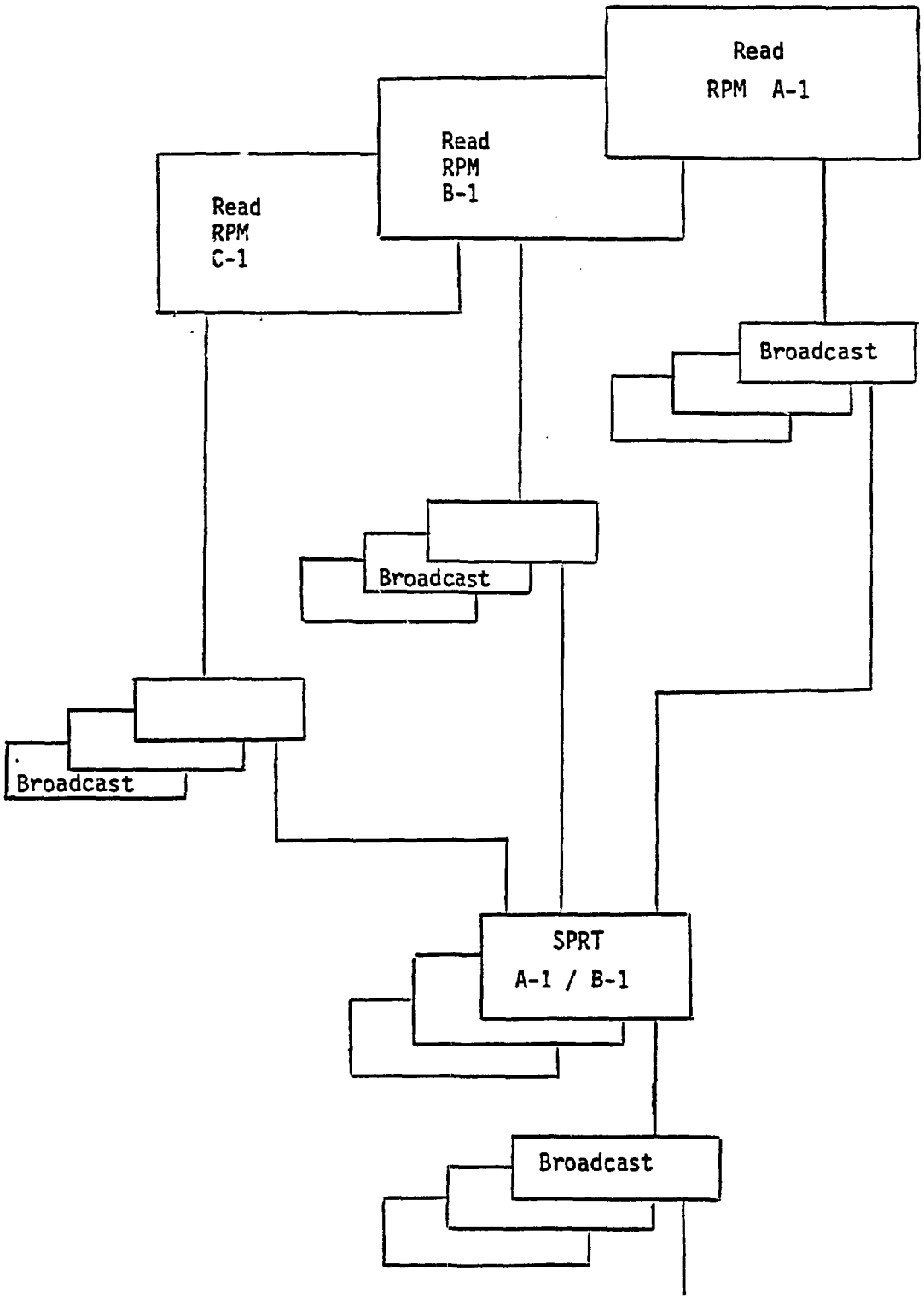


FIGURE 5 (CONTINUED)

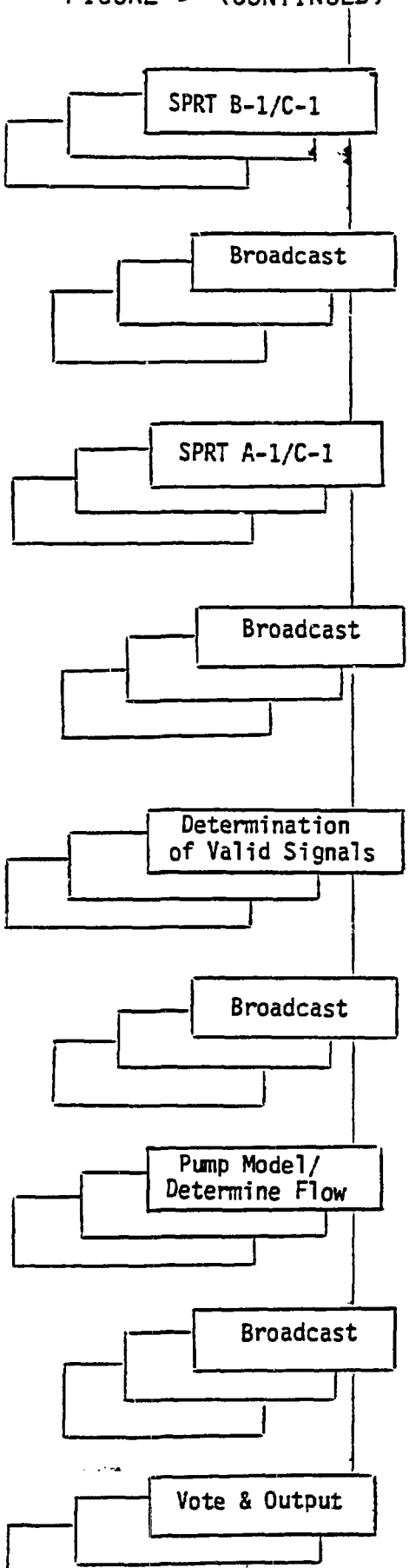
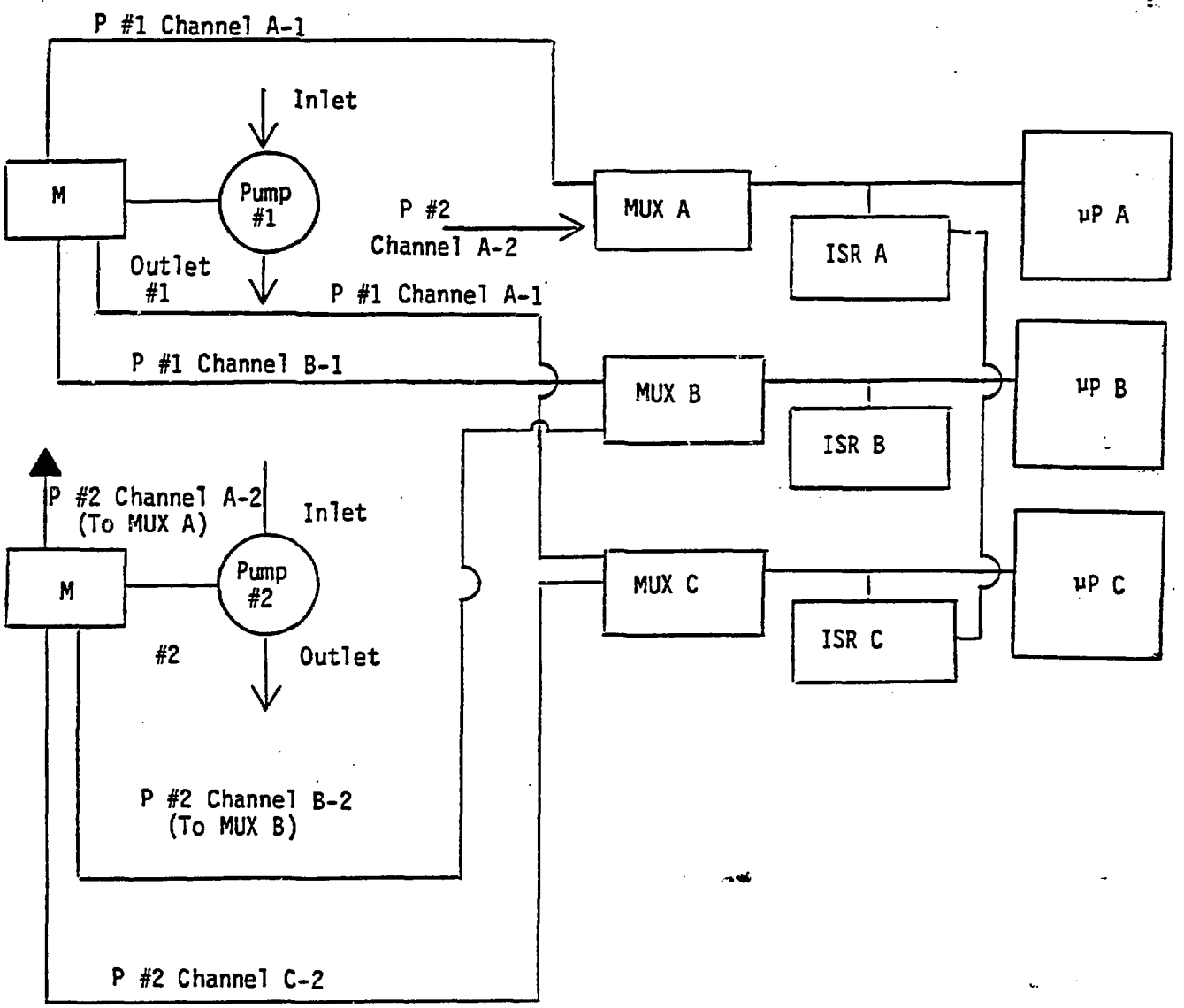


FIGURE 6



Symmetry "B" Hardware