CONF-841007--3

DESIGN STRATEGY FOR CONTROL OF INHERENTLY SAFE REACTORS*

by

Gregory H. Chisholm

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

Submitted for Presentation
at the
1984 Nuclear Science Symposium
October 31-November 2, 1984
Orlando, Florida

* Work Supported by the U.S. Department of Energy under Contract W-31-109-38.

DESIGN STRATEGY FOR CONTROL OF INHERENTLY SAFE REACTORS

G. H. Chisholm

Reactor power plant safety is assured through a combination of engineered barriers to radiation release (e.g., reactor containment) in combination with active reactor safety systems to shut the reactor down and remove decay heat. While not specifically identified as safety systems, the control systems responsible for continuous operation of plant subsystems are the first line of defense for mitigating radiation releases and for plant protection.

"Inherently safe" reactors take advantage of passive system features for decay-heat removal and reactor shutdown functions normally ascribed to active reactor safety systems. The advent of these reactors may permit restructuring of the present control system design strategy. This restructuring is based on the fact that authority for protection against unlikely accidents is, as much as practical, placed upon the passive features of the system instead of the traditional placement upon the PPS. Consequently, reactor control may be simplified, allowing the reliability of control systems to be improved and more easily defended.

Gregory H. Chisholm
(208) 526-7766

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.

DESIGN STRATEGY FOR CONTROL OF INHERENTLY SAFE REACTORS

G. H. Chisholm

SUMMARY

I. Introduction

An inherently safe reactor is herein defined as one which does not require active safety systems for decay heat removal or reactor shutdown. While the ideal may not be fully attained, it can be approached by many designs currently being proposed. The control strategy for an inherently safe reactor must recognize the shifting of safety responsibility from the reactor shutdown system to the passive features of the reactor system and should take full advantage of this change in safety design requirements. As an extension of this realization, the control system, assuming an improvement in reliability, could conceivably satisfy both operating and safety requirements. One would presumably retain a reactor safety system but its functions could be simplified and its actions limited to the extreme events.

II. Discussion

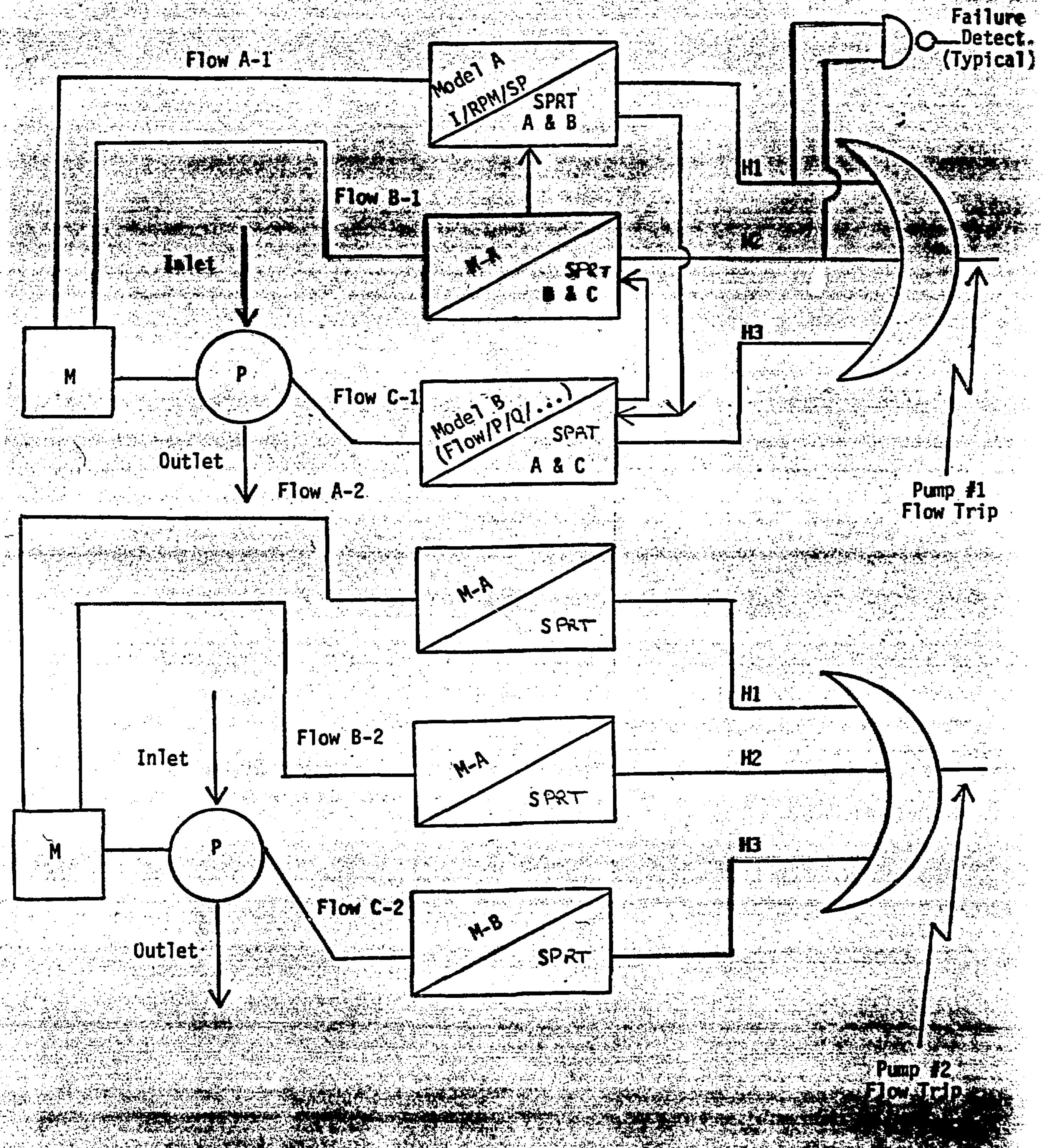
The design impact of placing upon the Control System (CS) the authority for protection of the reactor against anticipated events is the subject of this paper. The intention is to demonstrate the feasibility of a lead to design which could lead overall improvements in reliability and safety.

A control system could be considered analogous to an expert system, e.g., a control system detects differences between the process and the desired setpoint and takes action to bring the process within proper bounds. The suggested strategy requires the CS to perform its job with higher reliability and with additional expertise to ensure protection against anticipated transients. Increasing the controller's reliability would not be so difficult if it were not for the required increase in expertise. The latter implies the application of digital systems for which reliability predictions are presently difficult. The complexity of digital systems requires large manpower expenditures to determine reliability because of the potential failure sources of software, hardware and the integrating effect between the two. Software failures are insidious in that they belie correspondence with hardware failure predictions, i.e., a software bug exists until the process takes that specific path through the program. However, that path may not be taken but once in 10 years. Secondly, the software may suffer "lacks" which result from failure of the design specification to define a requirement. This second failure is common to hardware, but occurrences can be more dependent upon system complexity than system intrinsics.

The recent availability of fault-tolerant computers presents a potential problem solution to part of the reliability proble, i.e., the hardware reliability and software/hardware interaction. However, use of fault-tolerant computers typically requires the use of common software which opens the question of common mode failure. Alternatives are diverse software which operate either on the same or diverse machines. Cost benefits will ultimately determine the optimal approach. Additionally, the fault-tolerant properties of these systems must be demonstrated to meet reliability requirements. Currently, Markhovian analytical techniques are employed for this demonstration. Some work is being done to verify design claims utilizing automated reasoning. Acceptance of either technique will depend on a proper demonstration.

An overview of ongoing research concerning software reliability indicates that a multitude of approaches are being investigated. NASA is conducting experiments for hardware simulation, fault-tolerant computer operation, software reliability modeling and formal proofs via automated reasoning. Argonne National Laboratory (ANL) is involved in a pilot project directed toward developing automated techniques for system analysis. The Institute of Electrical and Electronic Engineers (IEEE) is involved in writing a guide for measurement of software reliability using approximately 60 metrics (measures). The U.S. Navy sponsored a project which resulted in development of an interactive program which incorporates eight of the existing models for software reliability measurement. Though a significant effort is being expended toward determination of software reliability, results must be considered preliminary. This caution suggests that diverse software coupled with the argument that simultaneous failures constitute an incredible event is the best approach for immediate applications. The proposed design strategy adopts this approach and is based upon utilization of fault-tolerant hardware. Rigid analysis is necessary to validate system claims for fault-tolerance and is the subject of research at ANL and NASA.

Figure 1 depicts a conceptual design for a computer based reactor safety system proposed for installation at the Experimental Breeder Reactor. The system will monitor pump parametrical data and derive flow from diverse models. Generic software will be utilized to support extension of technology developed by this project toward support of systems capable of reliable reactor control, i.e., control systems for which safety credit may be taken during the licensing process.



Symmetry - Functional Diagram