CONF-770737--1

FUNCTIONAL SAFEGUARDS FOR COMPUTERS FOR PROTECTION SYSTEMS FOR SAVANNAH RIVER REACTORS

W. R. Kritz

E. I. du Pont de Nemours and Company
Savannah River Plant
Aiken, South Carolina 29801

June 1977

Synopsis of a paper for IAEA Specialist Meeting on Software Reliability for Computerized Control and Safety Systems in Nuclear Power Plants. July 1977, Pittsburgh, PA.

This paper was prepared in connection with work under Contract AT(07-2)-1 with the U. S. Energy Research and Development Administration.

INTRODUCTION:

Reactors at the Savannah River Plant have recently been equipped with a "safety computer" system. This system utilizes dual digital computers in a primary protection system that monitors individual fuel assembly coolant flow and temperature. The design basis for the (SRP safety) computer systems allowed for eventual failure of any input sensor or any computer component. These systems are routinely used by reactor operators with a minimum of training in computer technology. The hardware configuration and software design therefore contain safeguards so that both hardware and human failures do not cause significant loss of reactor protection.

REDUNDANCY:

To provide a tolerance for normal failures, the 1200 input signals were divided between two computes as indicated in Fig. 1. Each computer has access to either flow or temperature data from each of 600 fuel assemblies. The computers are completely independent, with dedicated alarm and trip outputs. Reactor shutdown is initiated if neither safety computer is functional. This arrangement provides redundant protection for power excursions and general flow incidents, with non-redundant protection for for reduction in individual fuel assembly flows.

RESPONSE TIME:

Reactor shutdown is designed to be initiated with 0.5 seconds for flow reduction incidents, and within 1.0 seconds for power excursions. Scanning rates of 2000 and 1000 inputs/second respectively were selected for the analog flow and temperature signals to each computer to permit input verification before alarm or trip action. Solid-state scanners (multiplex-converter units) were designed and built to our specifications for this service.

To assure fast response to real process changes regardless of momentary computer workload, each input is compared to limits as it is read from the

scanners. Interrupt service routines, normally used only to maintain data tables in memory, were expanded to provide these monitoring functions. (Fig. 2) Service routines for the flow and temperature data:

1. Perform validity tests on each input,
2. Test good data against alarm and trip limits,
3. Pass alarm message parameters to an ALARM program to record input errors and abnormal reactor conditions,
4. Initiate reactor shutdown when a trip condition is confirmed,
5. Maintain bad input counters and declare the computer inoperative if preset limits are exceeded,
6. Maintain flag tables for automatic recovery from specific input faults,
7. Maintain tables of maximum and average temperatures; maximum, average and minimum flows.

These service routines require about 200 microseconds to process each new data input (Fig. 3), thus about 60% of the computer time is devoted to routine monitoring. All of the support programs share the remaining time at pre-selected priority levels.

An AUDIT program runs once per second to test for scan completion, and timely execution of automatic support programs. If any AUDIT test fails, the computer is immediately declared inoperative. The AUDIT program arms an external (watchdog) timer on satisfactory completion of all tests. This timer will also declare the computer inoperative if not re-armed within two seconds. (Fig. 4)

There are three reactor shutdown (trip) relay sets associated with the safety computers. Each computer can initiate reactor shutdown independently when a reactor incident condition is detected during interrupt service of flow or temperature data. The third set of trip relays monitors safety computer status

and initiates reactor shutdown on loss of safety computer protection. Any program can declare a safety computer inoperative. Hardware logic also declares a computer inoperative if (1) the watchdog timer fires, (2) the computer console is unlocked, or (3) the trip relays are bypassed.

DATA VALIDITY TESTS:

The scanners provide two test words (converter status and input sequence number) for each signal conversion. Any input is declared bad for incomplete conversion, hardware-detected conversion error, or an unexpected sequence number. A standard voltage is connected as the first input to each 8-channel multiplex card. If the converted standard signal fails to meet quality tests, the seven temperature or flow signals for that card are declared bad.

Special transducers (Fig. 5) were designed and fabricated to our specifications to provide tests for the flow data. Both outputs from a transducer are converted before scanner interrupt. The interrupt service routine declares the input bad if the sum of the dual signals is not within a narrow band of acceptable values. The difference between these signals is an accurate measure of differential pressure used to indicate coolant flow.

Unreasonable temperature data are rejected on the basis of possible conditons for liquid D_2O in the (SRP) reactors. Counters are maintained for bad temperature and flow inputs, and the interrupt service routines are disabled if preset limits are exceeded, thus making the individual computer inoperative.

CONFIRMATION OF POWER EXCURSION (Fig. 6):

Coincidence logic is used to confirm high temperature signals before initiating reactor shutdown. If a signal from one assembly exceeds the trip setpoint, reactor shutdown will be initiated if (1) either of the two adjacent assembly (confirming group) temperatures is above the alarm setpoint or (2) both of the temperature inputs from adjacent positions are bad. This technique permits repair to other

instruments that also access these thermocouple signals without unnecessary reactor shutdown or delay in safety circuit response to real power excursions. For non-uniform configurations with different kinds of assemblies in a reactor charge, alarm setpoints are specifically calculated for each reactor position and power distribution. The TSET program runs once per minute to perform this service.

Wiring arrangement was specified for the temperature scanner to support this coincidence logic with provision for input errors. The sequential scan selects the first input from a group of multiplexer cards before advancing to the second input for this same group of cards. The signals for three reactor assemblies in a confirming group are thus connected to three separate cards. This arrangement permits adjacent reactor positions to be monitored sequentially while preventing the loss of all temperature data from a confirming group as a result of a single multiplex card failure.

SOFTWARE PROTECTION: (Fig. 7)

All software for the safety computers is thoroughly tested, documented and approved before use during reactor operation (Reference 1). To maintain the integrity of this software during subsequent operation, several protective features are used. Copies of all software are maintained on protected disk tracks, and facilities are provided for push-button reloading, with automatic restart, if reactor operators have any reason to suspect that the operating software has been damaged. The total off-line time required for a safety computer restart is less than one minute.

Some of the protective features were purchased from Interdata, Inc., the computer manufacturer. These include standard features such as key-lock disabling of the computer console, privileged instructions that are permitted only in system-level software, and an anti-change feature in the OS/16-MT

operating system. Optional protective devices, including memory parity and partitioned memory protect controllers, were also purchased from Interdata.

Additional protection was provided by choice of location, additional hardware and software provided by our personnel. The safety computers are located in the reactor control rooms, in full view of operation personnel who are present at all times. Each computer console switch is wired to relays that declare the computer off-line unless the switch is locked.

An AUDIT program must run every second, and determine that the required data scans and automatic programs are performing on schedule, to prevent a "watchdog timer" from declaring the computer off-line. AUDIT also tests several words in the computer memory to protect against accidental changes. AUDIT, ALARM and other programs print messages for all detected abnormalities, and initiate audible and visual alarms to draw operator attention to the messages.

Special software devices were created for the data input and digital output devices used in the (safety computer) systems. These devices perform only those functions required for normal monitoring, and will refuse service to all programs other than the monitoring program to which each is dedicated.

RESULTS:

After 12 reactor-months of safety computer operation, we have demonstrated significant gains with the new equipment. Periods of inadequate monitoring had been experienced with the previous analog systems. These were caused by human error and prolonged by difficult testing methods, and have been eliminated. Reactor image has been increased by shorter setup time for new fuel charges and by fewer unnecessary shutdowns (Fig. 8).

We have had problems with reliability of electrical power, radio-frequency noise pickup from relay contacts in other reactor systems, and occasional transistor failures. Voltage surges on our power grid have caused reactor shutdown by driving both computers off-line at the same time. Relay noise has been responsible for spurious bad input alarms, even with extensive use of isolated wiring and radio-frequency shields. The average availability of each safety computer has been at least 98%, including shutdowns for replacement of circuit boards with faulty transistors, approved program changes, etc.

We believe that all of the protective features included in the (SRP) safety computers were necessary. Only greater experience will demonstrate whether the protection of the software is sufficient for our needs.

REFERENCES:

1. R. H. Finley, Programming of Computers for the Protection System for Savannah River Reactors, IAEA Softwear Specialist Meeting, Pittsburgh, Pa., July 1977. DPSPU 77-30-5 E. I. du Pont de Nemours & Co., SRP, Aiken, SC 29801

This paper was prepared in connection with work under Contract AT(07-2)-1 with the U. S. Energy Research and Development Administration.

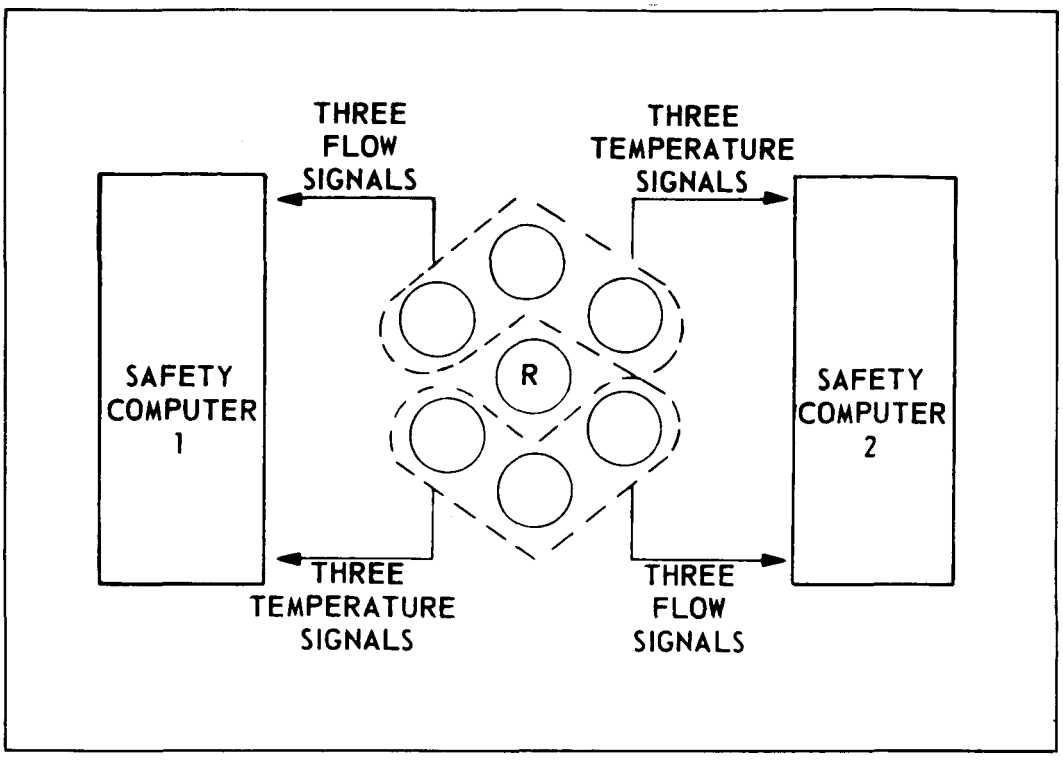

FIGURE 1. TYPICAL OF 100 SIX-ASSEMBLY GROUPS

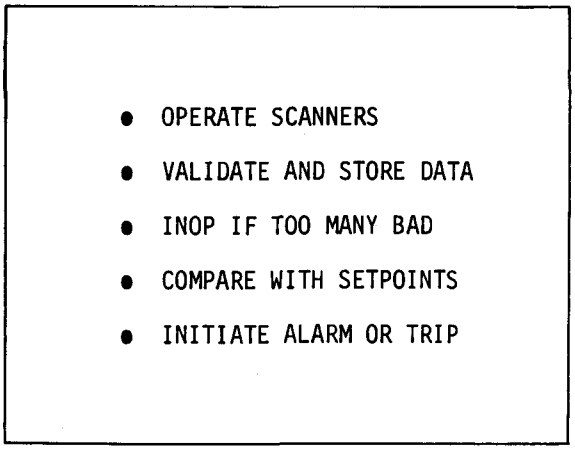

FIGURE 2. INTERRUPT SERVICE ROUTINE

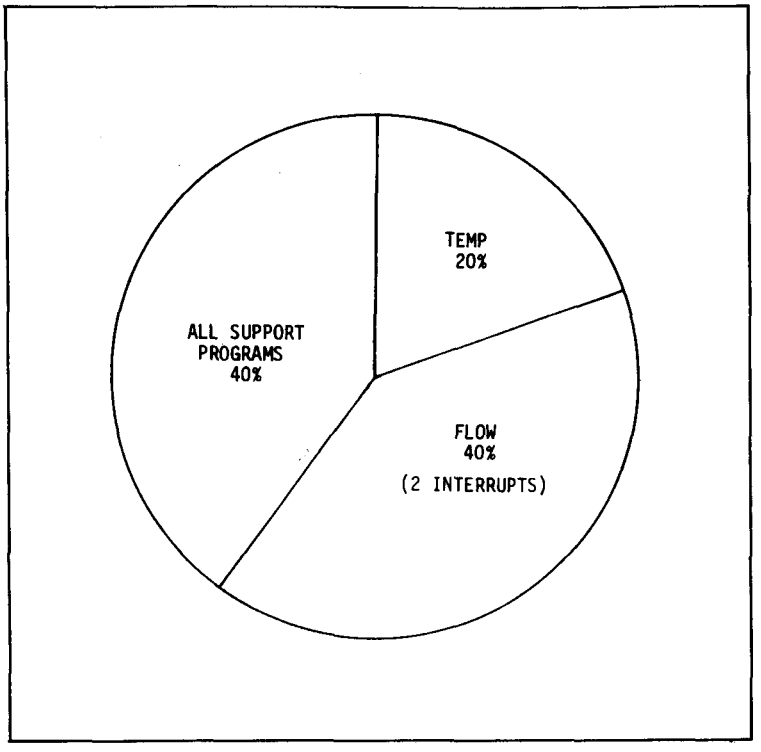

FIGURE 3. SAFETY COMPUTER WORKLOAD,
TYPICAL MILLISECOND

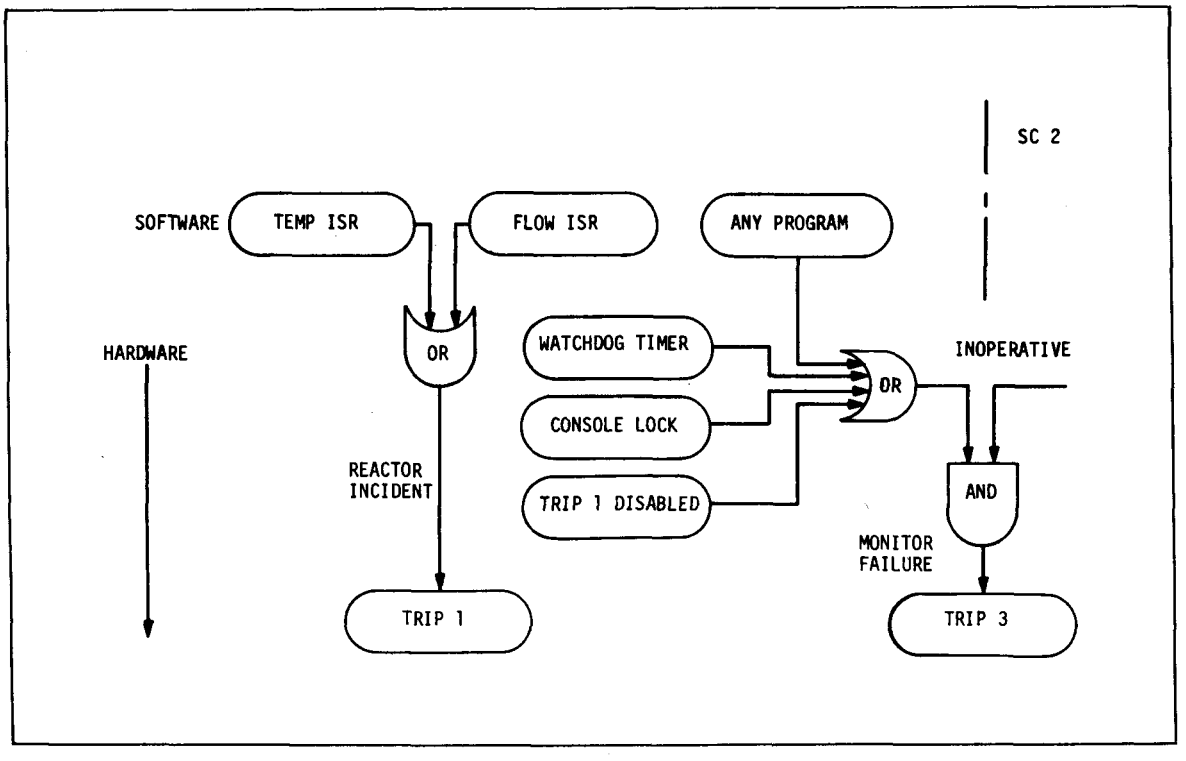

FIGURE 4. SAFETY COMPUTER 1

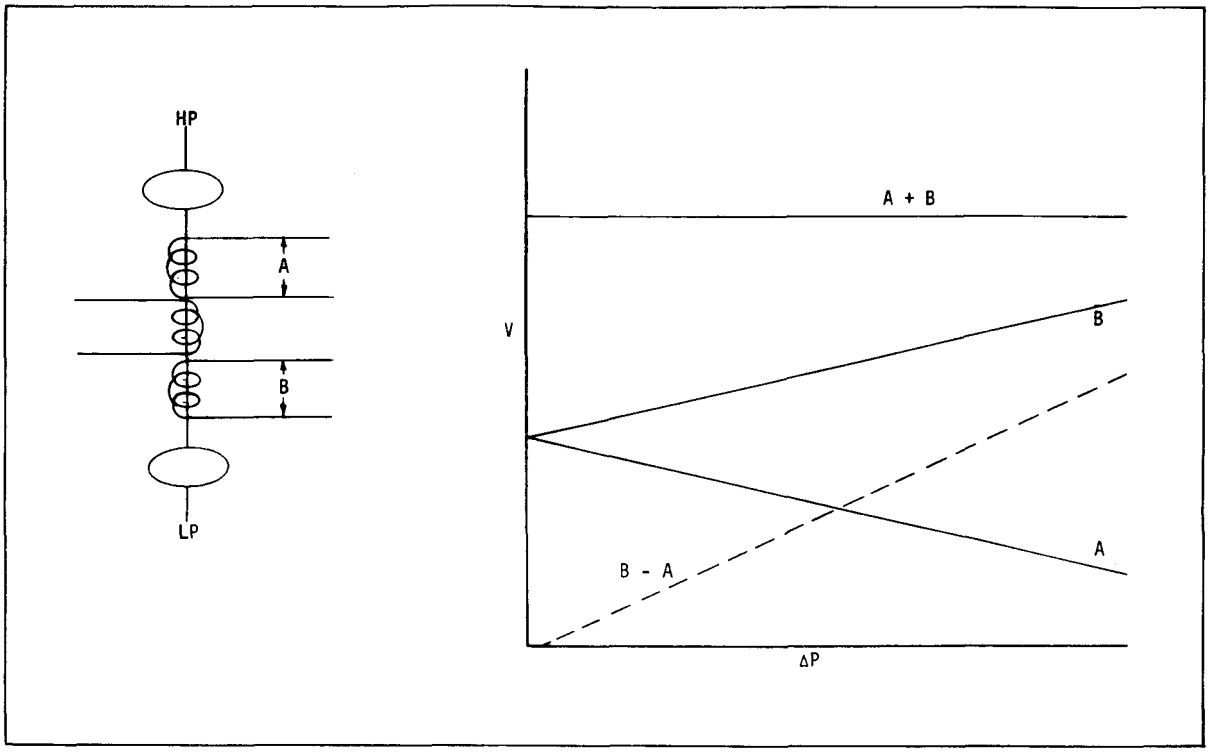

FIGURE 5. TRANSDUCER

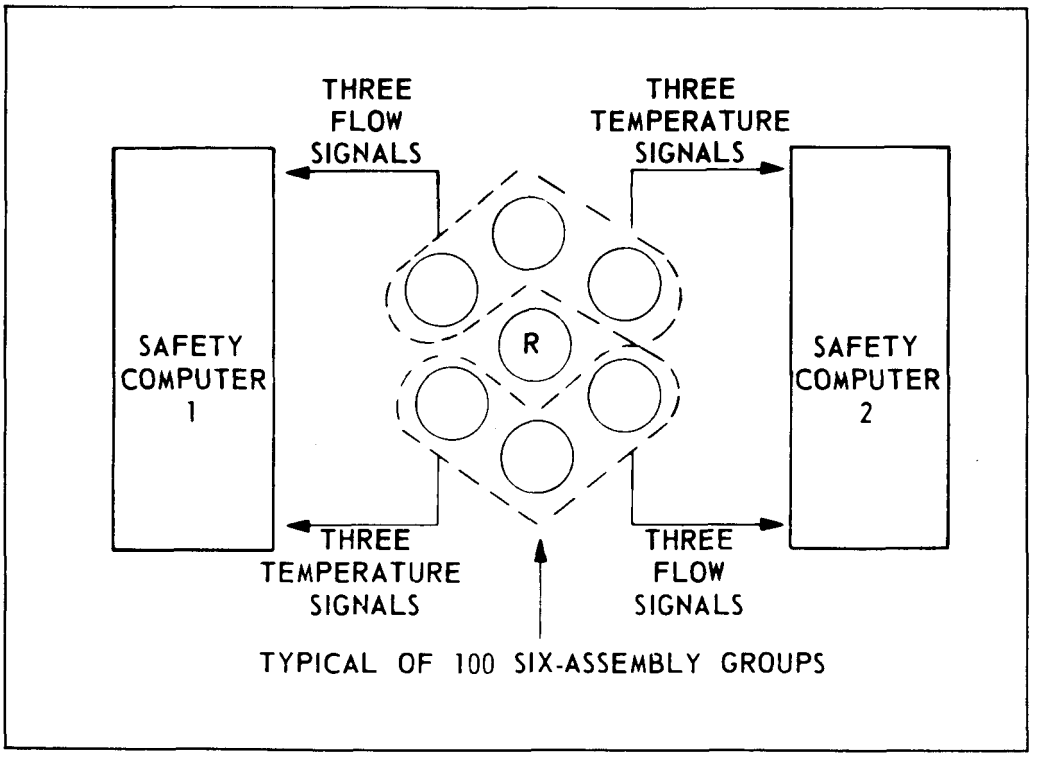

FIGURE 6. FLOW SIGNALS AND TEMPERATURE SIGNALS TO DUAL SAFETY COMPUTERS

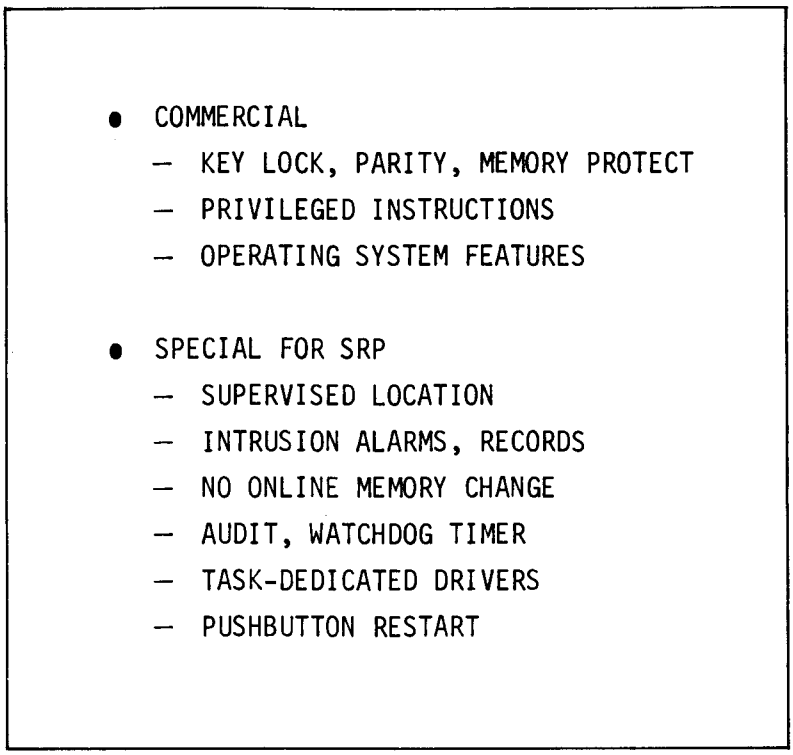

FIGURE 7. SOFTWARE PROTECTION

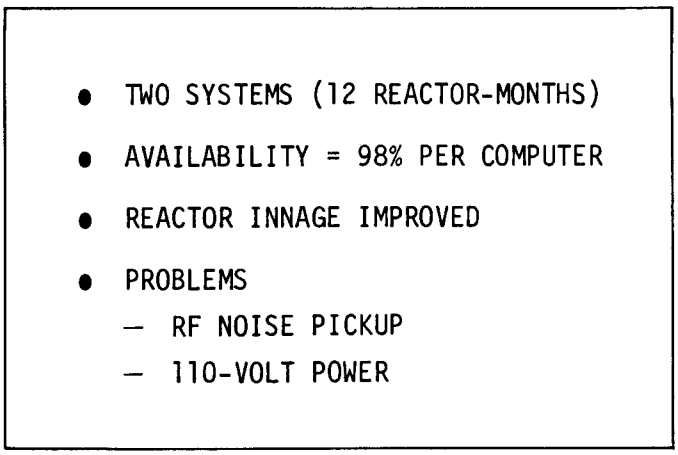

FIGURE 8. OPERATING EXPERIENCE