DPSPU 77-30-3

CONF-770708--2

USE OF DIGITAL COMPUTERS IN THE PROTECTION SYSTEM FOR SAVANNAH RIVER REACTORS

K. L. Gimmy

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

June 1977

To be presented at the ANS meeting on Thermal Reactor Safety at Sun Valley, Idaho, ~~August 1-4, 1977~~. 31 July - 5 Aug. 1977

MASTER

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

USE OF DIGITAL COMPUTERS IN THE PROTECTION SYSTEM FOR SAVANNAH RIVER REACTORS

K. L. Gimmy

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

SUMMARY

Each production reactor at the Savannah River Plant has recently been provided with a protective system using dual digital computers (slide 1). The dual "safety computers" monitor coolant temperature and flow in each of the 600 fuel assemblies in the reactor. The system provides alarms and automatic reactor shutdown (SCRAM) if these variables exceed predetermined setpoints. The system provides the primary protection for unwanted local or general power increase or assembly coolant flow reduction. Standard process control computers are used and all scanning, data output, and protective action are controlled by software prepared by Du Pont.

The system was designed to minimize the effect of single component failures. Each safety computer monitors flow signals from one-half of the reactor positions and temperature signals from the other half (slide 2). This arrangement provides either flow or temperature monitoring for the coolant to each assembly, even if one computer is bypassed or inoperative. Loss of both computers causes a reactor scram.

The major part of this paper deals with our approach to two problem areas that confront any large computerized protection system (slide 3).

1) How to ensure signal accuracy and proper response to real changes, but reject the spurious signals that are bound to occur with 1200 sensors.
2) How to develop and test computer software so that it will be at least as reliable as hard-wired logic circuits.

DISCUSSION

INPUT VALIDATION

Many techniques were used in the hardware and software to validate input signals. Individual coolant flows are measured by 600 differential pressure transducers with linear variable differential transformer (LVDT) output characteristics (slide 4). Each LVDT has two secondary windings and the two output signals are used for logical rejection of false data (slide 5). The difference in the two signals is proportional to the ΔP used to measure flow, but the sum of the two signals is a constant value. Any significant change in the sum indicates a problem with either the sensor, wiring, or the scanner. Similarly, programmed coincidence logic requires that a temperature increase in the coolant of one reactor assembly be confirmed by an increase in an adjacent assembly before a power increase is indicated. Each signal must pass a reasonableness test to be accepted. Any signal over a setpoint must persist for two scans, about a third of a second, to be believed. These techniques

(slide 6) effectively eliminate false scrams and alarms from sensor failures, multiplexer problems, or noise spikes of very short duration.

System calibration is routinely verified by several standard inputs whose voltages are known and are included in every data scan. This is a standard technique for process computer systems. But for this application it was expanded to provide a standard voltage input as the first input on each multiplexer circuit card (slide 7). Sacrificing one out of every eight inputs is expensive, but it is a good way to detect the signal averaging that can occur with solid-state scanners. If an input gate circuit fails in the ON condition, that signal may average with other signals. All signals on that card would be wrong but none might be degraded enough to be detected by the reasonableness test. By making the first input a known precision value, a very tight test of ±1% can be used on that input to detect averaging with another input. As a side benefit, various standard values were used so that the entire range of the input system calibration could be verified. Bad sensors or calibration errors are annunciated and if they exceed present limits, the computer goes offline.

SOFTWARE DEVELOPMENT

Twenty-one programs were prepared for the safety computer system. The actual monitoring is done by core-resident scan programs which handle a total of 3000 process signals per second. These interrupt-driven routines must of necessity be very short or they will consume all of the available processor time. Thus the scan routines compare and store only raw data. Programs that print or display data do the conversion to engineering units. Limit values are back-converted (with calibration offsets) to raw data format for scan usage.

With so much data flowing through the system, a method was needed to save sets of data that would be consistent when printed or examined. A HISTORY program systematically saves operating data each minute on a magnetic disk (slide 8). The data saved for each input consist of the maximum, the minimum, and the average for the minute. As the data grow older, only selected sets are retained and intervals between sets grow longer. Thus, the "minute" file would be used to investigate the cause of an alarm but the "shift" file would be examined to detect a slow trend. The HISTORY file has proven very useful to the reactor operators (slide 9).

A number of methods were used to improve the reliability of the software (slide 10). Much use was made of system security features such as memory protect boundaries, watchdog timers, and an independent auditing program. After normal debugging and integration into an operating system, a failure-response test was made. This detailed test used deliberately induced failures in the computer and inputs to force the software down seldom-used branches of the logic. Then a 30-day test of simulated operation was used as the final acceptance test of the software. Each program was documented in an approved abstract covering mathematics, limitations, and a logic flow chart.

OPERATING EXPERIENCES

Reactor operation with computers in the protection system has been smooth. The new safety computers have been more reliable and have caused fewer spurious shutdowns than the analog systems they replaced. A few software inadequacies have occurred but there were none that reduced the protective functions or that caused spurious action. Each half of the dual system has been online

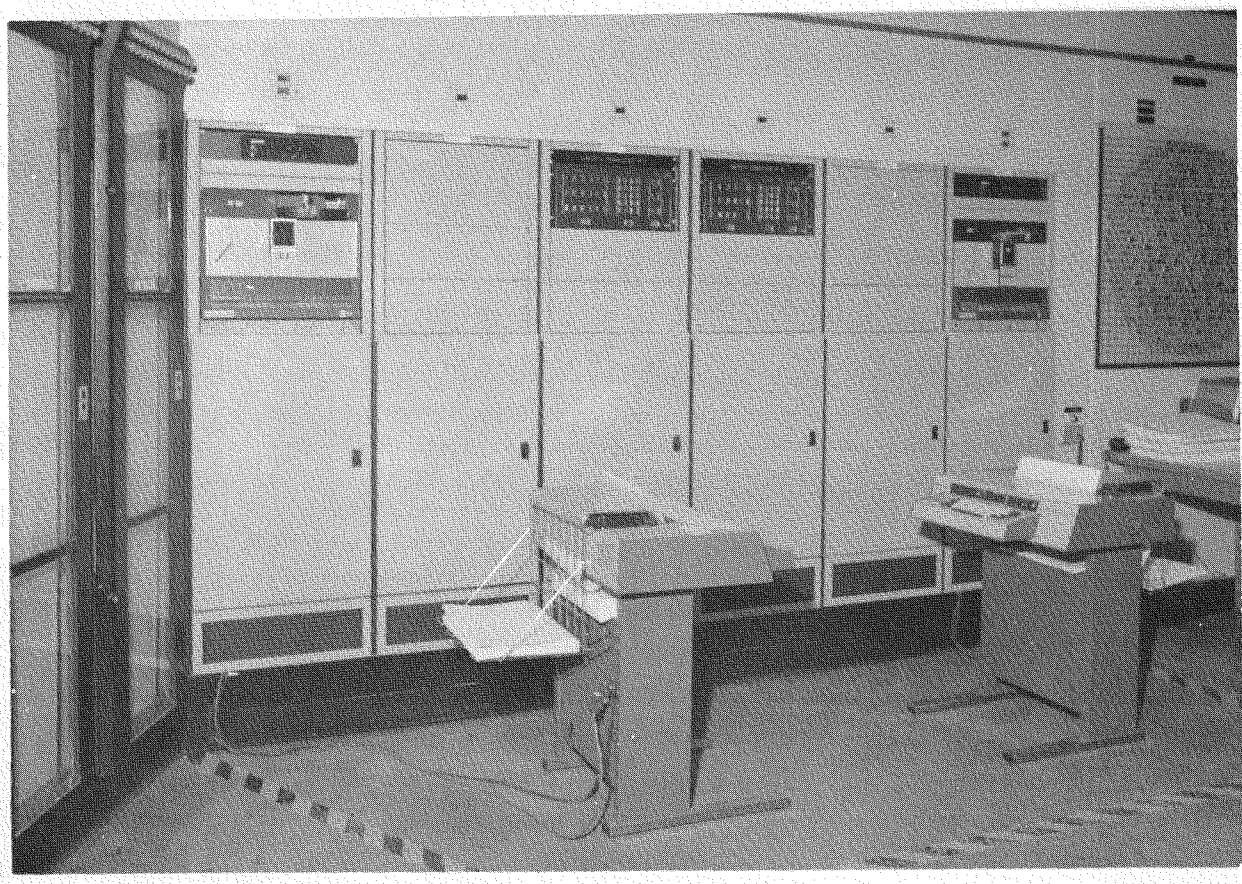
and unbypassed more than 98% of the time, including testing and maintenance. The system is maintained by the plant instrument group. Reliability data collected during 1 year of system testing and actual operation are summarized in slide 11.

REFERENCES

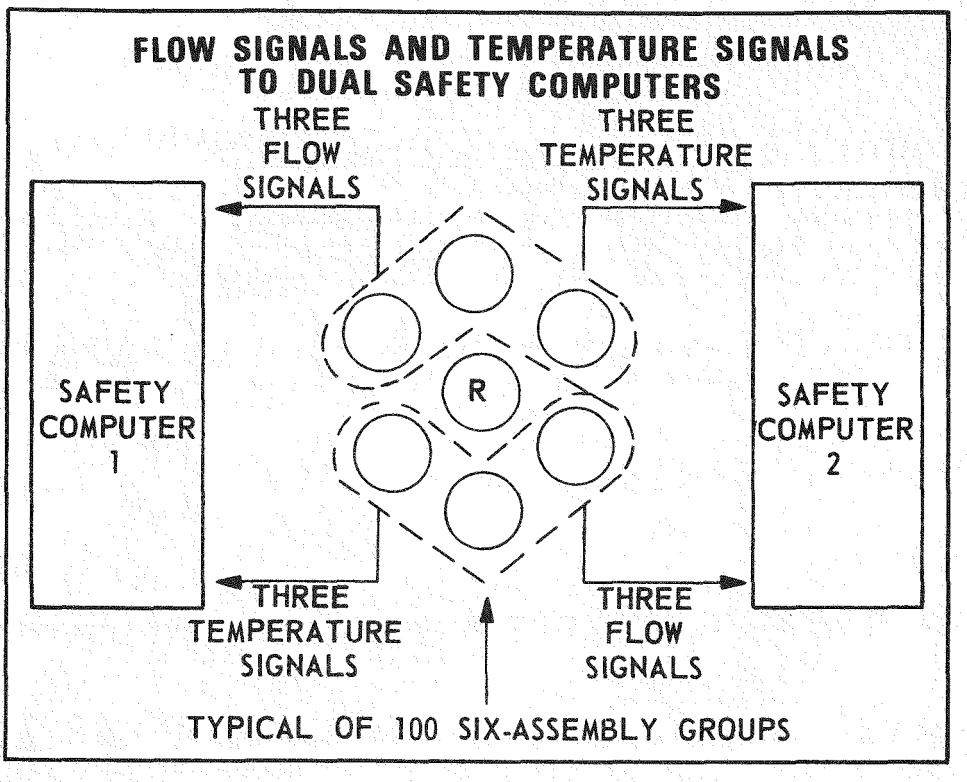
1. W. R. KRITZ, Functional Safeguards for Computers for Protection Systems for Savannah River Reactors. Paper for IAEA specialists meeting on "Software Reliability for Computerized Control and Safety Systems in Nuclear Power Plants," Pittsburgh, PA, July 1977. DPSPU 77-30-6, E. I. du Pont de Nemours and Company, SRP, Aiken, SC 29801.

2. R. H. FINLEY, Programming of Computers for the Protection System for Savannah River Reactors. Paper for IAEA specialists meeting on "Software Reliability for Computerized Control and Safety Systems in Nuclear Power Plants," Pittsburgh, PA, July 1977. DPSPU 77-30-5, E. I. du Pont de Nemours and Company, SRP, Aiken, SC 29801.

Information in this document was developed in the course of work under Contract AT(07-2)-1 with the U.S. Energy Research and Development Administration.



SLIDE 1

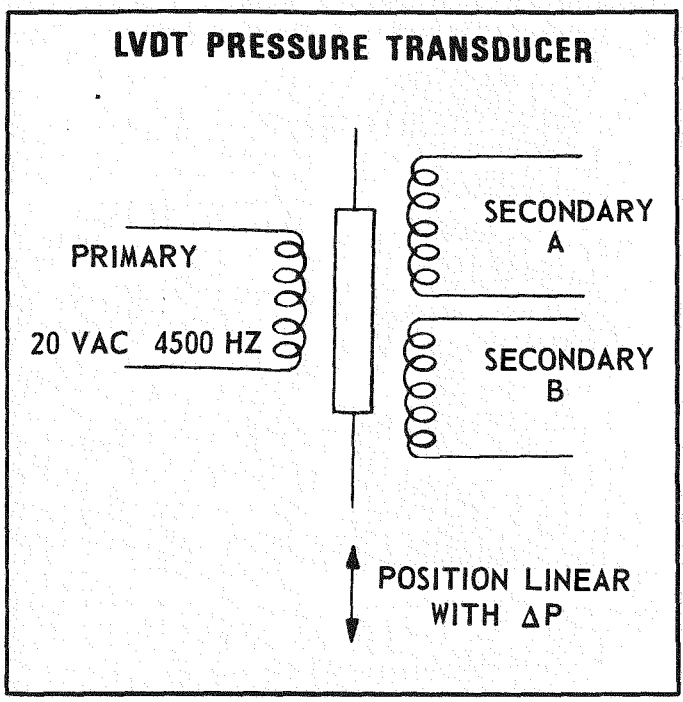


SLIDE 2

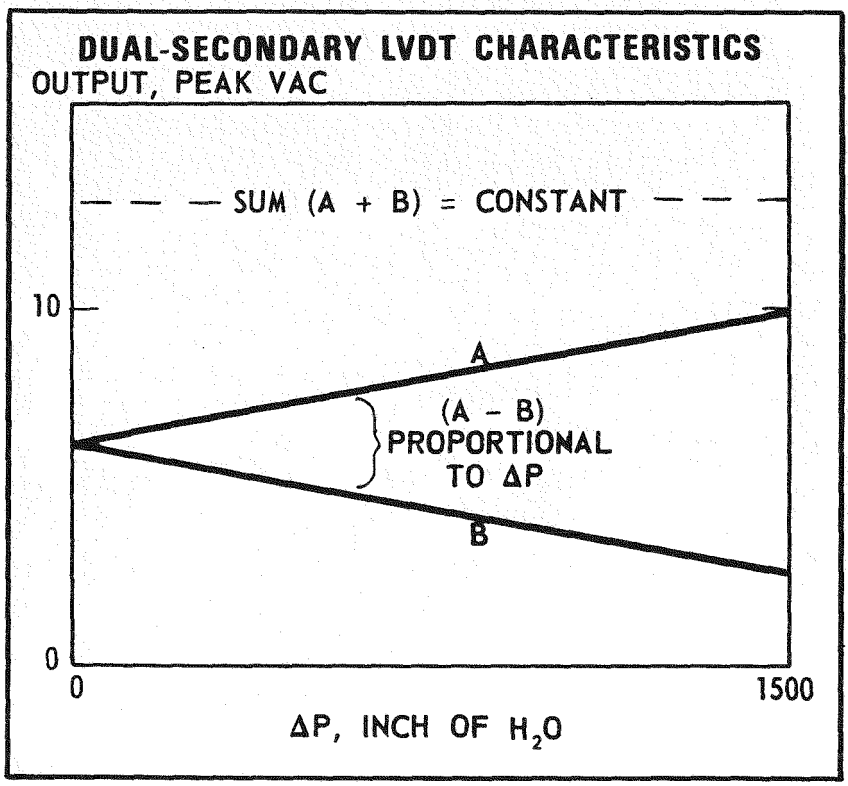
PROBLEM AREAS

1. HOW TO SCAN 1200 REACTOR SIGNALS
   - RESPOND TO REAL CHANGES
   - REJECT SPURIOUS SIGNALS
2. HOW TO DEVELOP RELIABLE SOFTWARE

SLIDE 3



SLIDE 4



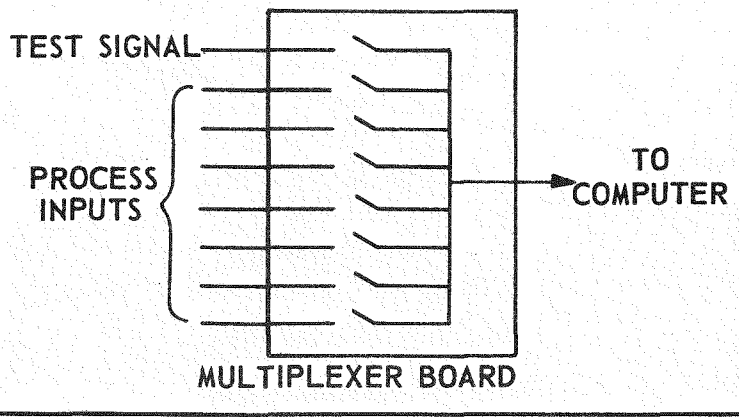
SLIDE 5

INPUT VALIDATION

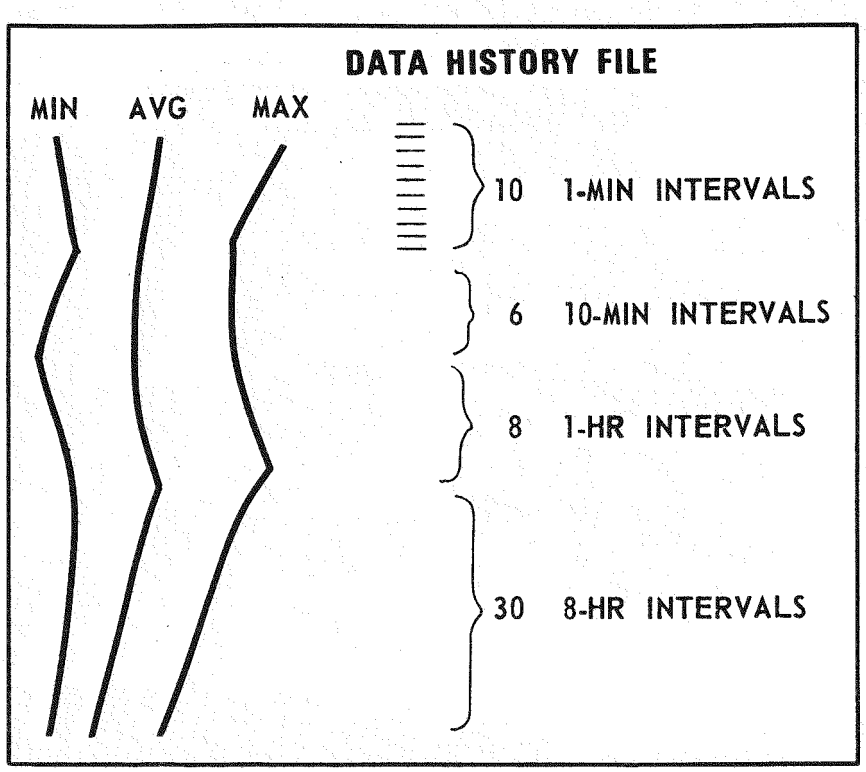
1. SUM TEST (FLOW)
2. CONFIRMING SIGNAL (TEMP)
3. REASONABLENESS
4. REREAD BEFORE ALARM
5. CALIBRATION TEST INPUTS

SLIDE 6

ONE "STANDARD" PER BOARD



SLIDE 7



SLIDE 8

HISTORY FILE USES

1. CONSISTENT DATA
2. DATA TRENDS
3. ALARM INVESTIGATION
4. SIGNAL NOISE ANALYSIS

SLIDE 9

SOFTWARE RELIABILITY

1. HARDWARE OPTIONS
2. DEBUGGING
3. FAILURE-RESPONSE TESTS
4. 30-DAY TEST
5. DOCUMENTATION

SLIDE 10

EQUIPMENT RELIABILITY DATA

	MTBF HOURS	% OF TOTAL UNITS REPAIRED IN ONE YEAR
INTERDATA MODEL 70 COMPUTERS	2000	9*
DATAWEST ANALOG SCANNERS (AC & DC)	1000	11*
PERIPHERAL DEVICES	-	56

* % OF TOTAL CIRCUIT BOARDS

SLIDE 11