CONF-841007--39

A MICROPROCESSOR TESTER FOR THE TREAT UPGRADE REACTOR TRIP SYSTEM

F. R. Lenkszus and R. G. Bucher
Argonne National Laboratory
Argonne, Illinois 60439

CONF-841007--39

DE85 004082

Introduction

The upgrading of the Transient Reactor Test (TREAT) Facility at ANL-Idaho has been designed to provide additional experimental capabilities for the study of core disruptive accident (CDA) phenomena.[1] To improve the analytical extrapolation of test results to full-size assembly bundles, the facility upgrade will increase the maximum size of the test bundle from 7 to 37 fuel pins. By creating a core convertor zone around the test location, the neutron spectrum incident on the test assembly will be hardened and the maximum energy deposited in the sample will be increased. In addition, a programmable Automated Reactor Control System (ARCS) will permit high-power transients up to 11,000 MW having a controlled reactor period of from 15 to 0.1 sec. These modifications to the core neutronics will improve simulation of LMFBR accident conditions. Finally, a sophisticated, multiply-redundant safety system , the Reactor Trip System (RTS), will provide safe operation for both steady state and transient production operating modes.

To insure that this complex safety system is functioning properly, a Dedicated Microprocessor Tester (DMT) has been implemented to perform a thorough checkout of the RTS prior to all TREAT operations. A quantitative reliability analysis of the RTS shows that the unreliability, that is, the probability of failure, is acceptable for a 10 hour mission time or risk interval. Consequently, an automated tester is necessary to complete the RTS checkouts and allow reactor operations within this restricted interval; it is expected that the complete RTS checkout sequence will require less than two hours. Additionally, the DMT will improve the reliability of the checkout by reducing the potential for gross human error; that is, the DMT will monitor the RTS to verify that the operator responded correctly to each DMT-requested action, e.g., to press a button. Therefore the DMT will both increase the efficiency of the RTS checkout and improve the reliability of the validation.

RTS Description

The basic function of the Reactor Trip System (RTS) is to protect the reactor facility by preventing potentially damaging uncontrolled reactivity excursions. The RTS monitors the facility for the occurrence of abnormal operating conditions by continuously comparing instrumentation signals against preset limits. Upon sensing an out-of-limits condition, the RTS initiates a reactor scram by removing the control-rod-drive latch voltage. The RTS is designed to monitor both steady state and transient production operations; bypasses are employed, as needed, to circumvent steady state trip circuits in the transient production mode. A comprehensive block diagram of the entire RTS is presented in Figure 2; the quantities in parentheses indicate the number of signals represented by the single line.

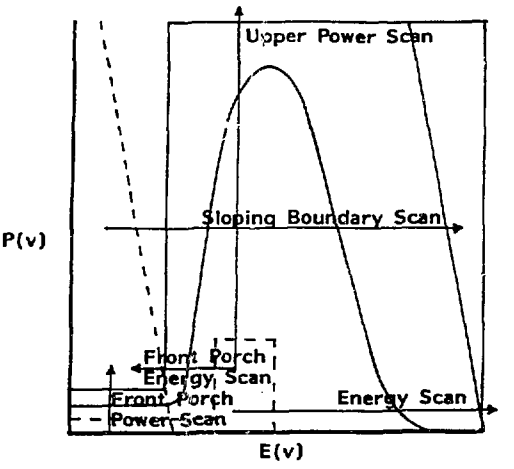

Figure 1a. Transient-Dependent Parameters for Transient Input Trip Logic (—— maximum, --- minimum)

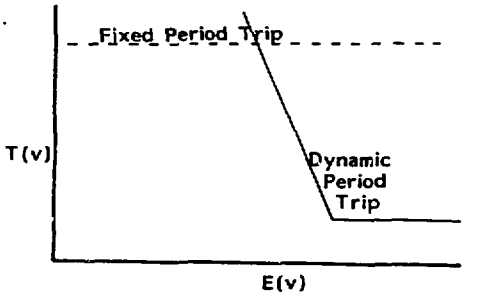

Figure 1b. Transient-Dependent Dynamic Period Trip

The RTS transient instrumentation is a triply-redundant system; each group, identified by A, B, or C, consists of Linear Power, Integrated Power or Energy, and Log/Period nuclear channels that deliver analog inputs to the Transient Input Trip Logic. The input trip logic compares these analog inputs to specified reference values which define the operational boundary for transient production. The boundaries for the power and energy signals are displayed on the power versus energy (PE) plane in Figure 1a, along with the trace of a typical transient; the scans indicated on the figure are discussed in Test Procedures. Two boundaries, and hence two separate trip circuits, are defined: one, the transient-dependent which is adjustable using 10-turn potentiometers on the front panel and, two, the transient-independent which is internally hard-wired.

DISCLAIMER

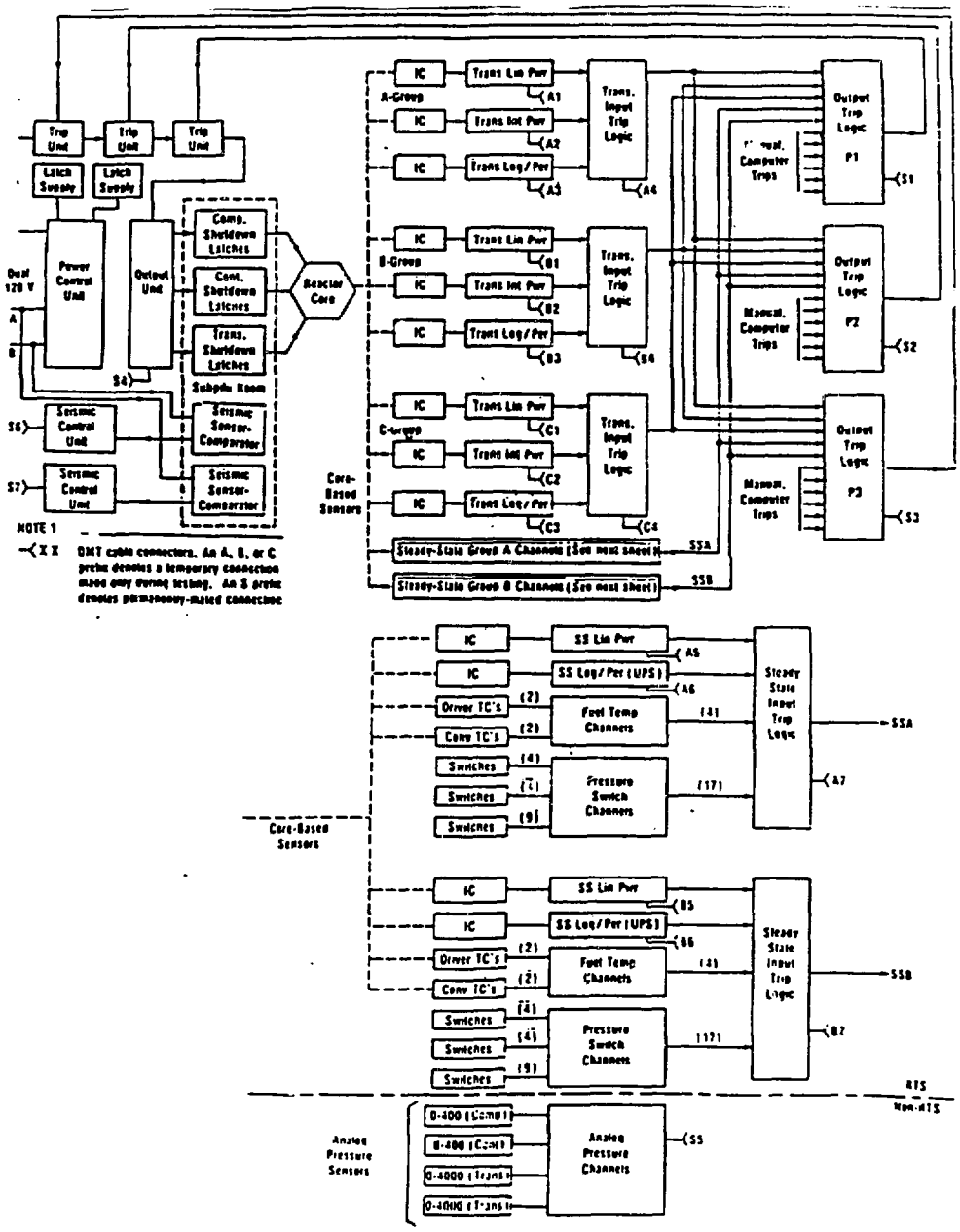

Figure 2. RTS Block Diagram

The maximum values for the transient-dependent boundary correspond to those for the transient-independent boundary; therefore, the transient-independent trip circuits serve as backup to the transient-dependent trip circuits. Similarly, the period signal has both dependent and independent boundaries and corresponding trip circuits. In addition, the transient-independent circuits include a dynamic period boundary which provides an energy-dependent period trip point. The boundaries for the dynamic period trip are displayed on the time versus energy (TE) plane in Figure 1b.

The RTS steady state instrumentation is a doubly-redundant system; each group, identified by A or B, consists of Linear Power and Log/Period nuclear channels as well as Fuel Temperature and Pressure Switch channels that deliver analog and digital inputs to the Steady State Input Trip Logic. As with the transient instruments, the function of the input trip logic is to compare the inputs to specified reference values. The analog power, period, and fuel temperature inputs are compared with adjustable limits set via front panel potentiometers; the digital pressure switch inputs are monitored continuously to insure the control rod drive pressure exceeds the minimum operational limits.

The latched trip-status outputs from the five Input Trip Logic units, together with trip signals from the ARCS computers and manual scram buttons, are input to each of the triplicated Output Trip Logic units. If one of these units senses the tripped-condition on any of its inputs, it signals the solid state relays in the corresponding Trip Unit to turn-off. Since the Trip Units are in series, turning-off the relays will remove the latch power from all control rod drives, thus scramming the reactor. Additionally, two independent seismic channels will initiate a scram if the ground acceleration along any of the axes in the subpile room exceeds limits.

DMT Implementation

DMT Hardware

Figure 3 is block diagram of the DMT hardware. Since the DMT is an extension of the TREAT Upgrade Automatic Reactor Control System (ARCS), it uses commercially available hardware compatible with the ARCS. The DMT's CPU is an 8086/8087 Multibus* single board computer. Additional Multibus boards provide 216 bits of digital I/O, 64 multiplexed channels of 12-bit analog input, and 8 channels of 12-bit analog output. The DMT distribution panel is the physical interconnect between RTS/DMT cables and the DMT I/O ports. The distribution panel provides passive R-C filtering on all analog and digital inputs and interfaces RTS bi-directional analog signals with the DMT analog to digital converter (ADC) and digital to analog converters (DAC). CMOS switches controlled by DMT digital outputs are used to connect and disconnect the DMT digital to analog converters. In addition, the distribution panel provides 2 reference voltages used in the DMT's ADC calibration self-check.

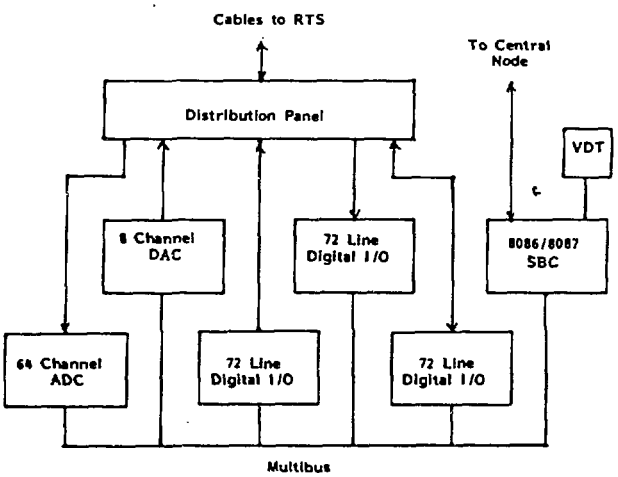

Figure 3. DMT Block Diagram

The DMT connects to the ARCS central node computer via a serial port. The DMT uses this link to the central node to obtain printer services, to invoke ARCS initiated stimuli, and to obtain nonvolatile storage. Since the DMT is not configured with a printer, it must use the central node's line printer to generate hardcopy of test results. Text is sent via the serial port to a print task running on the central node. The DMT is required to test the RTS response to ARCS initiated stimuli such as computer trips and transient enabling signals. The DMT requests operator invocation of these ARCS initiated stimuli by sending a message via the serial port to the central node task. Finally, the DMT requires writable nonvolatile storage for core configuration dependent parameters. Since the DMT has only PROM and RAM memory, it must use the Winchester disk on the central node to store and recall core configuration dependent parameters. Again this is accomplished through communications with a central node task via the serial port.

DMT Software

The DMT software system uses Intel's IRMX88* executive. IRMX88 is PROM-based, event-driven and multitasking. All applications code for the DMT is written in Intel's PLM86 high level compiling language. The code is generally structured into a program, subprogram and module organization. Basic functions such as analog and digital input and output are at the module level. These modules are invoked by subprograms to test individual instruments. The subprograms in turn are invoked by the DMT RTS test task which performs testing of the RTS.

Figure 4 graphically depicts the DMT's software task organization. At power-on or reset IRMX88 creates and starts the initialization/null task. This task in turn creates exchanges required for intertask communications, initializes flags and variables, and creates and starts the time, terminal, and communications tasks. The time task measures elapsed time with a one millisecond resolution. The terminal task handles communications with the DMT console by using exchanges to communicate with the IRMX88 terminal driver. The communications task, which provides communications with the central node via the serial port, actually consists of two tasks, a communications input task and a communications output task. These tasks communicate via exchanges with interrupt service routines which interact with the serial port to effect transfers.

The terminal task operates in either of two modes, data entry or command entry. In data entry mode, operator console input is passed via an interface routine to the requesting routine. The interface routine simplifies programming by handling the message interchange between the communications task and the requesting routine. A routine needing operator console input calls the interface routine with buffer pointer and maximum count parameters. The interface routine sets the terminal task mode to data entry, forms a message and sends it to the terminal task and then waits at a response exchange. The communications task upon receipt of operator input from the terminal handler via the terminal handler response exchange, forms the operator input into a message and passes it to the interface routine. The interface routine then moves the operator input to the buffer pointed to by the buffer pointer parameter, restores the terminal task to command entry mode, and returns to the requesting routine.

In the command entry mode, the terminal task processes operator console input received from the terminal handler as DMT commands by passing the input through a command line interpreter. Upon recognition of a legal DMT command, the appropriate command handling procedure is invoked. Legal DMT commands are

* Multibus and IRMX88 are trademarks of Intel Corp.

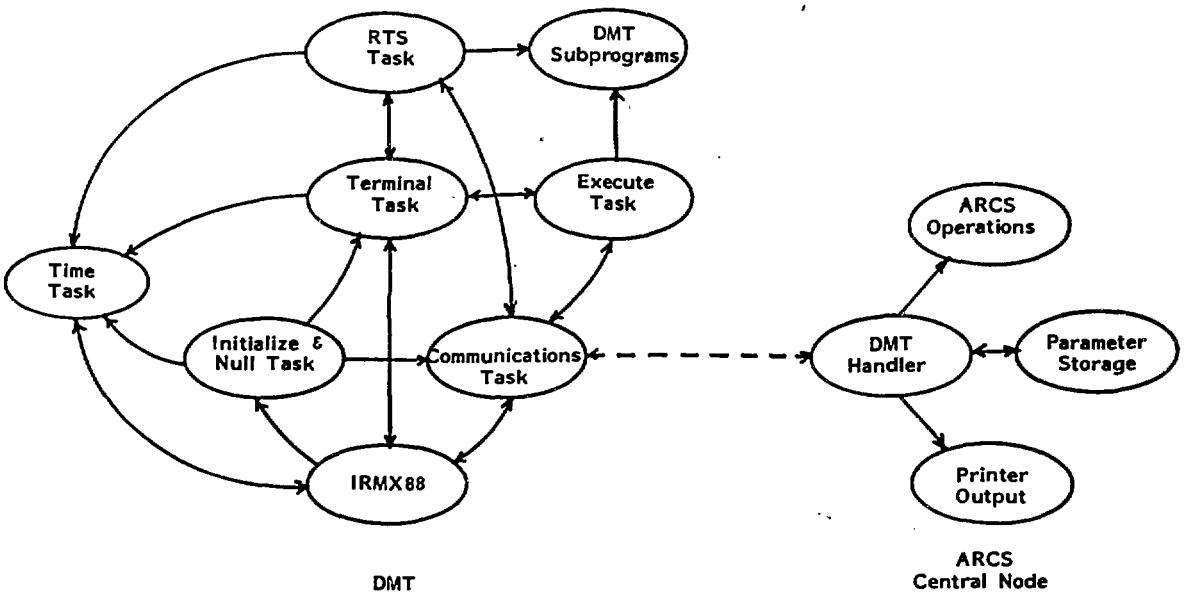

Figure 4. DMT Software System

Start, Abort, Pause, Continue, Setup, Help, Repeat, Time, Execute, and Acknowledge. Setup is used to specify items such as enable and disable output of hardcopy test results on the central node's line printer. Start is used to initiate a complete test of the RTS and to begin elapsed time counting. Upon recognition of a Start command, the terminal task creates and starts the RTS test task which executes the RTS test procedure. The Execute command causes the terminal task to create and start the execute task which performs a single step of the RTS test procedure. Because it allows the selective execution of a single DMT step, the Execute command is particularly useful during RTS maintenance, test, and calibration. Abort, Pause and Continue respectively kill, suspend or resume the RTS test or execute tasks. The Time command displays the time elapsed since issuance of the Start command. The Repeat command causes the last DMT step specified in an Execute command to be repeated. The Acknowledge command is used to signal the DMT that a DMT requested operator action has been completed.

Since integrity of the DMT is crucial to proper testing of the RTS, the DMT executes self tests immediately prior to and subsequent to RTS testing. The tests check PROM, RAM, anslog-to-digital (ADC) and digital-to-analog (DAC) converter calibration, and the distribution panel CMOS switches. PROM contents are verified by comparison of a computed checksum with a checksum stored in PROM. The readability, writability and addressability of RAM is checked with a sliding ones and zeroes test. The ADC calibration is checked at three points against references within the distribution panel. The calibration of each DAC is checked against the ADC at two points by looping each DAC output back to the ADC, outputting values to each DAC, reading each DAC's output with the ADC and comparing the result to limits. The distribution panel's CMOS switches are checked through a procedure of applying voltages with the DACs and monitoring response with the ADC while the switches are operated in a prescribed sequence.

In normal operation prior to transient production, the Setup command is used to enable hardcopy output of test results on the central node's line printer. The Start command is then issued to initiate the RTS test procedure and begin counting elapsed time. The DMT then verifies its integrity by executing its self tests. Upon successful completion of the self tests, the DMT requests the operator to enter the date, time, core identification and operator identification. The RTS test procedure commences upon operator confirmation that the requested information is correct. During execution of RTS test procedure, the Pause and Continue commands may be used to suspend and resume RTS testing. Pause does not affect the counting of elapsed time. Each page of the DMT output identifies the instrument under test, the tests performed, the allowable limits for each test result, and the test results. Each page of the test results displays the date, the core id, a consecutive page number, the elapsed time since test initiation, and a valid or invalid test indicator. Each page is marked valid until a failure occurs. When a test result is out-of-limits, the out-of-limits result is printed with a failure message and marked with a flag. In addition, the current page and each subsequent page of the test result printout is marked invalid to signal that a failure has been detected. Operational procedures require the RTS test procedure to be executed from start to finish without a detected failure. Thus when failures are detected, the causes must be corrected and the entire RTS test procedure repeated. Execution of the entire test without failure is necessary to ensure that a corrective action has not inadvertently compromised a part of the RTS tested prior to a failure.

Test Procedures

The methodology of the test procedures is primarily the application of an external stimulus followed by the observation of the system response. Two techniques are employed to assert the initiating stimulus. In the first, the DMT automatically initiates the stimulus either by enabling a test circuit within the instrument or by injecting an external signal into the instrument's circuits. In the second, the DMT requests the operator to initiate the stimulus, e.g., by pressing a button, and to acknowledge that the action has been completed; when possible, the DMT verifies that the requested action was properly executed. If necessary, the DMT also examines the state of the instrument prior to the applying the stimulus to insure that all applicable trip circuits have been reset and that the correct operating modes have been established. Two segments of the test procedure have been chosen to illustrate the methodology; these are discussed in the following paragraphs.

STEP: 500 DATE: 10/26/84
MODE: TU CORE: TEST-000

TRANSIENT LINEAR CHANNEL TESTING - GROUP A

RANGE SWITCH VERIFICATION:
CONFIRM RANGE = 1e-3 . ENTER C TO CONFIRM; ALL ELSE TO REPEAT.)) C
CONFIRM RANGE = 1e-4 . ENTER C TO CONFIRM; ALL ELSE TO REPEAT.)) C
CONFIRM RANGE = 1e-5 . ENTER C TO CONFIRM; ALL ELSE TO REPEAT.)) C
CONFIRM RANGE = 1e-6 . ENTER C TO CONFIRM; ALL ELSE TO REPEAT.)) C
CONFIRM RANGE = 1e-7 . ENTER C TO CONFIRM; ALL ELSE TO REPEAT.)) C
CONFIRM RANGE = 1e-8 . ENTER C TO CONFIRM; ALL ELSE TO REPEAT.)) C
CONFIRM RANGE = 1e-9 . ENTER TO CONFIRM; ALL ELSE TO REPEAT.)) C

TEST	RANGE	VALUE	HI LIMIT	LO LIMIT	UNITS	OUT OF LIMITS
SUM 15 VDC		0.714	0.744	0.684	VOLTS	
PLUS 5 VDC		5.003	5.010	4.989	VOLTS	
BACKGROUND	1e-9	0.001	-----	1.250	VOLTS	* * * *
ZERO CHECK	1e-3	0.001	0.003	-0.003	VOLTS	
1e-3 A CAL	1e-3	9.004	9.036	8.963	VOLTS	
1e-4 A CAL	1e-4	9.001	9.036	8.963	VOLTS	
1e-5 A CAL	1e-5	9.004	9.036	8.963	VOLTS	
1e-6 A CAL	1e-6	9.007	9.036	8.963	VOLTS	
1e-7 A CAL	1e-7	8.992	9.001	8.918	VOLTS	
1e-8 A CAL	1e-8	8.993	9.540	8.440	VOLTS	
LIN PWR CAL GAIN SETTING	1e-4	2.956	2.963	2.946	-----	

PAGE NO: 05 * * INVALID * * ET: 00:02:20

Figure 5. Testing of RTS Transient Linear Channel

The first example, the testing of the Transient Linear Channel, is typical of the checkout of the steady state and transient nuclear channels. The printout from this test is shown in Figure 5. The initial portion verifies the capability of the DMT to select the instrument range. To accomplish this, the DMT sets up each range and requests the operator to confirm this setting by visual inspection of range indicator on the instrument. The second portion contains the checkout of the power supplies, the background current, the zero of the output, and the calibration of each range. Each test requires selecting the appropriate range and subsequently reading the channel output; the calibration tests also require the enabling of the internally-generated calibration current. The printout from these tests includes the instrument range, the value of the channel output, the acceptance limits for this output, and the units for these values. If the value is not within the acceptance limits inclusive, the test is flagged (* * * *) and the instrument test is marked invalid. The final test, the LIN PWR CAL GAIN SETTING, measures the gain of an adjustable amplifier in the Transient Input Trip Logic unit; this gain is compared to the configuration-dependent value which had been predetermined and saved on the central node's Winchester disk.

STEP: 3130 DATE: 10/26/84
MODE: TU CORE: TEST-000

TRANSIENT INPUT TRIP LOGIC TESTING - TRANSIENT DEPENDENT CIRCUIT - GROUP A

RESET IS PROPER.

ENTER FRONT PORCH VALUE, 377 TO 1256 MJ.)) 1000
FRONT PORCH VALUE = 1000 MJ, P1 = 8.000 V.

ENTER FRONT PORCH TRANSITION, 942 TO 1466 MJ.)) 1000
FRONT PORCH TRANSITION = 1000 MJ, E2 = 2.439 V.

ENTER UPPER POWER VALUE, 2513 TO 11353 MJ.)) 10000
UPPER POWER VALUE = 10000 MJ, P3 = 8.000 V.

ENTER ENERGY VALUE, 1909 TO 4100 MJ.)) 4100
ENERGY VALUE = 4100 MJ, E4 = 10.000 V.

ENTER SLOPE CONSTANT (MAX E AT P=0), 1025 TO 4100 MJ.)) 3000
SLOPE CONSTANT = 3000 MJ, T5 = 7.317 V.

ENTER C TO CONFIRM INPUT; ALL ELSE TO REENTER.)) C
SET ADJUSTMENTS P1, E2, P3, E4, T5, AND ACKNOWLEDGE.

SCAN TEST	VALUE	HI LIMIT	LO LIMIT	UNITS	FAILURE OR OUT OF LIMITS
FRONT PORCH POWER TRIP	8.007	8.090	8.070	VOLTS	
FRONT PORCH ENERGY TRIP	2.430	2.449	2.429	VOLTS	
UPPER POWER TRIP	8.009	8.010	8.79	VOLTS	
ENERGY TRIP	10.007	10.010	9.989	VOLTS	

SCAN TEST	SAMPLED VALUE,VE	COMPUTED VALUE,VS	HI LIMIT	LO LIMIT	UNITS	FAILURE OR OUT OF LIMITS
SLOPING BOUNDARY TRIP	6.396	7.319	7.417	7.217	VOLTS	

ENTER PERIOD TRIP VALUE, 1.000 TO 0.075 SEC.)) .8
PERIOD TRIP VALUE = 0.800 SEC, T6 = 0.250 V.

ENTER C TO CONFIRM INPUT; ALL ELSE TO REENTER.)) C
SET ADJUSTMENT T6 AND ACKNOWLEDGE.

SCAN TEST	VALUE	HI LIMIT	LO LIMIT	UNITS	FAILURE OR OUT OF LIMITS
PERIOD TRIP	0.254	0.259	0.239	VOLTS	

PAGE NO: 10 VALID ET: 00:00:03

Figure 6. Testing of Transient-Dependent Circuits of Transient Input Trip Log

The second example, the testing of the transient-dependent circuits of the Transient Input Trip Logic described in RTS Description, presents an excellent example of the DMT injecting signals into the instrument's circuits. The printout from this test is present in Figure 6. At the beginning of this test, the operator enters the boundary parameters for the transient, as prompted by the DMT. The DMT converts these physical parameters into voltage levels which the operator sets via the front panel potentiometers.

When the input parameters have been confirmed and the voltage settings have been acknowledged, the DMT begins execution of a series of voltage scans to test the transient-dependent trip circuits and, if the circuit is functioning properly, to measure the actual trip points. Each scan consists of inserting a fixed voltage on either the power or energy input of the trip circuits while applying a voltage ramp to the other input; see Figure 2a. By monitoring the state of the appropriate trip bistable, the DMT can determine the point on the voltage ramp at which the trip occurred. This trip point is compared to the appropriate voltage levels computed from the input boundary parameters; if the measured trip point is not within the acceptance limits, it is flagged (* * * *) and the instrument test is marked invalid. Note that an adjustment to the measured sloping boundary trip is required since the scan is executed at a power voltage different than that specified for the parameter input. The transient-dependent period trip value is also entered and tested by scanning the period signal.

Verification and Validation

Since the DMT is deemed to be "safety related", a quality assurance plan for the DMT implementation was written which conforms to the requirements of ANSI/ASME standard N45.2-1977, Quality Assurance Program Requirement for Nuclear Facilities. The QA plan spawned a number of control procedures addressing areas such as hardware and software design control, software development control, system test control, document control, etc.

Software verification and validation is an integral, significant factor in the DMT software design, development and testing process. A detailed software specification down to the module level was developed and verified against DMT functional requirements. Software development began after review and acceptance of the specification. Verification during the development phase consisted of review of module and subprogram listings and testing of modules and subprograms.

DMT system testing consists of system verification, validation, reverification, and revalidation phases. The verification and validation phases will be performed with the DMT's program in RAM rather than PROM to facilitate correction of any software problems. In the verification phase the DMT is required to successfully complete a test of an RTS system known to be error free. The validation phase consists of performing an error-seeded test to demonstrate the DMT's ability to detect and announce RTS failures. Approximately 300 errors will be sequentially seeded in the RTS to exercise all the DMT's fault detection capabilities.

Upon successful completion of the verification and validation tests, the DMT program will be committed to PROM and software configuration control will commence. The software configuration control requires the documentation of software problems in Software Problem Reports (SPR's) and the documentation of corrective actions or modifications in Software Change Orders (SCO's). An SPR identifies the nature of the problem, the conditions under which the problem manifested itself and the name and version number of the module causing the problem. After review of the SPR, an SCO is generated which specifies a software change, the purpose of the change, the module to be changed, the new module version number, the programmer to make the change, the date the change was made and the date the change was tested. The SPR's and SCO's provide an auditable trail of software changes.

After the DMT's program is transferred to PROM, the verification and validation tests will be repeated for the PROM resident version (reverification and revalidation) to ensure that the transfer has not introduced problems.

Conclusion

The DMT is currently undergoing testing with individual RTS units as they become available. DMT system testing (verification and validation) will begin in late November when the full RTS becomes available. The DMT is scheduled to be shipped to TREAT in mid February of 1985.

Reference

[1] C. E. Dickerman, et. al., "Upgrading of TREAT Experimental Capabilities," Proceeding Fast, Thermal, and Fusion Reactor Experiments, vol. 1, pp. 1-130, Salt Lake City, Utah, April 12-15, 1982.