LA-UR -81-1943

CONF-810630--10

TITLE: REDUNDANT CONTROL SYSTEMS FOR TSTA

AUTHOR(S): JOHN J. DAMRAN

MASTER

SUBMITTED TO: Dr. Shlomo Karni
Dr. Peter Dorato
Department of Electrical and Computer Engineering
University of New Mexico
24th Midwest Symposium on Circuits and Systems
Albuquerque, NM

June 29-30, 1981

University of California

LOS ALAMOS SCIENTIFIC LABORATORY
Post Office Box 1663 Los Alamos, New Mexico 87545
An Affirmative Action/Equal Opportunity Employer

Form No. 836 R3
St. No. 2029
12/78

UNITED STATES
DEPARTMENT OF ENERGY
CONTRACT W-7405-ENG. 36

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

EBG

REDUNDANT CONTROL SYSTEMS FOR TSTA

John J. Damran
Los Alamos National Laboratory
Los Alamos, NM 87545

ABSTRACT

The Tritium Systems Test Assembly (TSTA) is a Los Alamos National Laboratory facility being constructed for the purpose of developing, demonstrating, and interfacing technologies required in the deuterium-tritium fuel cycle of future fusion reactor systems. The control of the facility is performed by the Master Data Acquisition and Control System (MDAC). The MDAC employs eight computers in a multi-redundant configuration ensuring both the safe and reliable operation of the facility and a high degree of system availability. To accomplish this task, MDAC is separated into two isolated branches, one designated as the process branch and the other as the safety branch.

1. INTRODUCTION

The Tritium Systems Test Assembly (TSTA) is dedicated to the development, demonstration, and interfacing of technologies related to the deuterium-tritium (DT) fuel cycle for fusion reactor systems. The TSTA will consist of a large gas loop that can simulate the proposed fuel cycle for a fusion facility. The gas loop will be designed to handle up to approximately 500 moles per day of DT. The tritium fuel component is an isotope of hydrogen with a mass of three. Tritium is radioactive and has a half-life of 12.3 years, decaying by emission of a beta partical of 5.6-keV average energy. This material has a relatively high specific activity of 10,000 Ci/g. Because of its short half-life, tritium is not an abundant isotope which in turn contributes to its expense ($10,000/g).

The principal objectives for TSTA can be rather concisely stated.

A. Demonstrate the fuel cycle for fusion power reactors.

B. Develop, test, and qualify equipment for tritium service in the fusion energy program.

C. Develop and test environmental and personnel protective systems.

D. Provide a final facility that can be used for demonstration and as an example that could be directly copied by FED/INTOR*.

E. Demonstrate long-term reliability of components.

F. Demonstrate long-term safe handling of tritium with no major releases or incidents.

G. Investigate and evaluate the response of the fuel cycle and environmental packages to normal, off-normal, and emergency situations.

A very significant goal at TSTA will be to demonstrate that the flow rate and total quantity of tritium in a fusion reactor can be handled safely on a routine basis. The TSTA will serve as a base-line facility that will provide a large data base that can be used to establish future guidelines and requirements for fusion facilities.

The control of the TSTA facility is performed by the Master Data Acquisition and Control System (MDAC). The MDAC must perform a broad range of functions for the operation of TSTA under severe requirements for safety and availability. The requirement for safety is paramount in view of the large inventory (200 g) of radioactive tritium contained within the process loop of TSTA. This paper describes a data acquisition and control system

*Fusion Energy Device/International Tokamak Reactor

configuration that implements multi-redundant hardware to ensure the safe and reliable operation of the facility and to provide a high degree of system availability.

2. MASTER DATA ACQUISITION AND CONTROL SYSTEM

2.1 MDAC SYSTEM REQUIREMENTS

The main objectives of the Master Data Acquisition and Control System are to accurately measure performance parameters and to provide control of components, subassemblies, and the TSTA as a whole; to provide alarms for "out of limit" processes and conditions; to provide a redundant method to measure, control, and display critical parameters; and to ensure adequate safeguarding and accountability of records of the large tritium inventory.

The secondary purposes of the MDAC are the following.

A. Perform real-time data reduction and display.

B. Provide status of equipment via CRT graphics display.

C. Record all monitored information as a permanent data base.

D. Provide system simulation.

E. Develop software for control of TSTA (off line).

F. Perform off-line data reduction.

G. Provide a print-out of all alarms and resulting system/operator actions.

H. Study tritium damage effects and determine long term reliability of a wide variety of instrumentation and controls.

I. Assist in check-out of TSTA systems and components.

J. Provide and maintain preventive maintenance and history records for TSTA.

2.2 MDAC SYSTEM GENERAL DESCRIPTION

The Master Data Acquisition and Control System's hardware configuration consists of a Data Acquisition Subsystem (DAS), a Process Control Subsystem (PCS), a Man-Machine Interface Subsystem (MMI), a Computer Subsystem (CSS), and a Software Subsystem (SSS). A block diagram of the hardware subsystems and the interfaces between them is shown in Fig. 1.

The two minicomputers within MDAC act as the main process computers and are interfaced to the DAS, PCS, and MMI. Two of MDACs microcomputers are used as safety machines to override commands given by the process computers that would lead to an unsafe condition within TSTA and to provide safety-related information to the MMI dedicated to the safety branch of MDAC. The DAS and PCS are integrated subsystems and contain four microcomputers identified as front-end controllers. The remaining equipment in the DAS and PCS consists of a collection of transducers and controllers, interconnecting cabling between these units and major DAS equipment components and an assemblage of major equipment components used for conditioning, formatting, and interfacing TSTA measurement and control parameters to the CSS. Table I depicts a summary of the measurement and control parameters required by TSTA .

2.3 MDAC SYSTEM DESIGN

2.3.1 Process Branch

The block diagram of Fig. 2 shows the computers' interfaces to the DAS and PCS subsystems, which, in turn, interface to the TSTA process. The figure shows an important aspect of MDAC, that being the independent isolated branch of the data acquisition and control subsystems which is dedicated to monitoring the safety status of TSTA and taking corrective action regardless of the condition of the rest of the control system.

The two CPUs in the process branch (CPU-1 and CPU-2) are Data General Eclipse C330 minicomputers. Minicomputer No. 1 is the main process control, status display and data archiving computer that oversees the complete operation of the TSTA facility and CSS subsystem. It will also act as a back-up for the front-end controllers described later.

Because the process computer has access to all of the data concerning TSTA (including safety related parameters), it can potentially detect departures from normal operation long before they reach a level that could be considered dangerous. In some instances, a combination of small departures may be early warning signals of an impending dangerous situation. Therefore, the process computer will alert the operator of such trends in order that the operator may take corrective action.

Larger departures from normal operation are classified as "Alarms," in which case the process computer will take automatic corrective action including total shutdown of the facility if conditions are severe enough to be dangerous. In the event tritium is somehow released into the facility, the process computer will direct emergency clean-up operations automatically. These safety-related functions of the process computer are meant to be the first line of defense against an accidental malfunction. The safety computers described later provide an independent system of safety operation.

The major peripherals connected to CPU-1 are a system console, magnetic tape recorder, communications chassis, and a 196-megabyte disk. The CPU has 750 kbytes of memory and will run a multipurpose operating system (AOS).

The configuration of CPU-2 and its associated peripherals are identical to that of CPU-1. This minicomputer will normally be available for off-line data analysis, system simulation, and for software development. A secondary role of this minicomputer is to act as the process control computer when minicomputer No. 1 is unavailable because of scheduled or unscheduled maintenance. Of course, all of its previously assigned tasks must cease for the duration of this replacement.

In order to be able to assume control, this CPU's data base must be kept current. This task will be fulfilled in two ways. First, very current data will be transferred to CPU-2 from CPU-1 over an intercomputer link called a multi-processor communications adapter (MCA). Second, information will be obtained from memory modules whose content is maintained jointly by the process computer and the front-end controllers. These memories, which are part of the DAS, are located within the CAMAC* equipment described later and are accessible from either minicomputer.

Minicomputers CPU-1 and CPU-2 are interfaced to the process branch of the data acquisition and control subsystems via a system master crate. A system master crate is a standard CAMAC crate used to house units employing the CAMAC dataway structure as a communications channel between computer interface modules, a controller, normal user modules, and IEEE STD 596-1976 branch drivers. A priority arbitration circuit in the computer interface modules and system crate controllers allows only one CPU at a time to have control of a CAMAC cycle. This feature allows either minicomputer to have control of the interface and, in turn, the process automatically and without operator intervention. This type of interface accommodates a "hot" transfer from one minicomputer to the other should a malfunction in one be diagnosed, and a reconfiguration of the CSS is performed.

There are four microcomputers in the DAS and PCS subsystems of the process branch. As stated earlier, these microcomputers are

* Computer Automated Measurement and Control

referred to as front-end controllers, and each perform data acquisition and control functions for a discrete group of TSTA subsystems. These computers are Digital Equipment Corporation LSI-11s with 28 k of memory and have 512 kbytes of floppy disk storage each. A single printer console switchable between the four microcomputers will be used as the system console.

The data acquired by each microcomputer is stored in a CAMAC memory module associated with the respective microcomputer. The data is then transferred to CPU-1 or CPU-2 as applicable at a predetermined rate. These microprocessors will also perform control over their respective TSTA subsystems as directed by the minicomputer assigned the task of being the main process control computer.

As stated earlier, should a front-end controller fail, the process control minicomputer will assume the functions of the failed unit. Conversely, should the process minicomputer fail, the front-end controllers will sustain the TSTA process in a steady-state condition for a preselected time interval while the computer subsystem is being reconfigured and the back-up minicomputer is acquiring control of TSTA. This action can be accomplished because the front-end controllers are configured as CAMAC auxiliary controllers. Being auxiliary controllers, they can be interfaced to as many as six crates and provide control of the modules in those crates as shown in Fig. 3. The primary control of each crate is performed by the type-A2 crate controllers, which are in communication with the host computers (CPU-1 and CPU-2) through the system master crate. An arbitration circuit in the type-A2 crate controller allows either the host computer or the front-end controller (microcomputer) to have control of the modules in the crates. At present, the process section of MDAC has two parallel CAMAC branches as specified in IEEE Standard 596-1976. Each CAMAC branch has six crates. There are two microcomputers used as auxiliary controllers (front-end controllers) in each CAMAC branch.

The analog signals from the facility are brought into the control room and routed either to the appropriate signal conditioning/calibration circuit or directly to a multiplexer. The routing of these parameters is done by way of a patch board system. Those parameters that interface to the TSTA process loop and other critical parameters are patched to the signal conditioning/calibration cards and then to a single-ended multiplexer and twelve-bit analog-to-digital converter. The remaining analog measurements are patched to a differential multiplexer that incorporates a single instrumentation amplifier for signal conditioning prior to the twelve-bit analog-to-digital converter. Figure 4 depicts the block diagram of the integrated DAS and PCS subsystem and its interface to the process computers.

2.3.2 Safety Branch

Referring again to Fig. 2, the safety branch of the data acquisition and control subsystems is shown as an independent arm of MDAC. The two computers in the safety branch are LSI-11/23s and are identically configured with 128 k of memory and a 10-megabyte disk. Each unit will have a dedicated system terminal and operate under the RT-11 software operating system.

If both of the safety computers are functional, one will be assigned the roll of the safety computer, while the other will be available for use as a development machine for all safety computer and front-end controller software. In the event of failure of the primary safety computer, the alternate microcomputer will then take over the safety computer role. Each safety computer is interfaced to a CAMAC system master crate that provides the same functionality as does the system crate for the process computers. Again, an arbitration priority circuit enables only one safety computer at a time to have access to a CAMAC cycle.

The block diagram of the data acquisition and control subsystems of MDAC dedicated to the safety system is depicted in Fig. 2. The configuration as shown here features a redundant capability to handle emergency conditions brought about by hardware or software failure in either the process or safety branch of MDAC. The provision of alternate routes for the sensing of critical TSTA parameters and the provision for totally independent control modules to execute safety-related functions is a major aspect of the MDAC design. The control functions within the safety branch include the ability to isolate any of the TSTA subsystems, to completely shut down the facility, and to control the emergency tritium clean-up system of TSTA independently. Serial communication links are provided for between the CAMAC sections of the process and safety branches of MDAC. These communication links will be used primarily for diagnostic health checks of the equipment in the two branches (process and safety). These communication links will be discussed in more detail later.

The data acquisition and control equipment used in the safety branch of MDAC is identical to those modules used in the process branch. The analog signals to the safety branch are routed to the multiplexers and twelve-bit analog-to-digital converters from the patch board system. The signals to both the process and safety multiplexers come from the same sources. However, isolation of the process and safety systems is preserved by using resistor isolation, as shown in Fig. 5. In addition, those parameters deemed critical to safety are measured using three transducers, with both systems receiving all three signals. At present, this approach appears safer, more reliable, and less costly than a sophisticated software approach that would compare a parameter with several others to determine its authenticity.

The signals from the three transducers will be compared, and the transducer providing the signal closest to the average of the three signals will be used for control and/or display purposes. When one unit exceeds an error-band window, the operator would be notified of this anomaly, and that transducer would no longer be used in the signal averaging process or for a control/display signal. The signal from each redundant transducer will be patched to a different multiplexer and analog-to-digital converter. This configuration will circumvent a loss of critical data should a failure of one of these units be experienced.

The digital input signals patched to the safety branch are the same as those measured by the process branch (originate from the same switch, valve, etc.). Again, the integrity of the signals is maintained by providing resistor isolation between the two branches. The isolation is a natural fallout of the design of the input registers as the pull-up resistors and the resistors internal to the IC chips are used to obtain the required isolation. Figure 6 illustrates this feature.

The analog control signals from the digital-to-analog (D/A) converters in the two branches are isolated using relay contacts. Figure 7 depicts this configuration. The analog control signal from each system's D/A converter is wired to a relay whose normally closed contacts connect the process D/A converter to the appropriate controller by way of the patch board system. Should an anomaly be detected in the ability of the equipment in the process branch to provide adequate control, the safety computer will switch the relay and provide control using its D/A converter

To obtain override control of critical valves and switches, relay output isolation is achieved as depicted in Fig. 8. The process branch maintains control of the device until a failure is detected within that branch. At that time, the safety branch may exercise control of the device by toggling its output

register relay to achieve the desired position/condition of the controlled device. This action can be achieved since the safety branch also has access to the feedback signal from the controlled device.

2.3.3 System Intercommunication

Figure 9 illustrates the communication paths between computers in the process and safety branches of MDAC. Data may be passed between CPU-1 and CPU-2 in the process branch over the multiprocessor communications adapter (MCA) at a rate of 625 kbytes/s. As stated earlier, this path will be used to keep the data base of the standby computer current. It will also be used as a state-of-health check for CPU-1 and CPU-2.

The mailbox memory associated with each front-end controller will be used for state-of-health checks as well as passing data. This action will verify the health of all the interfaces from the main process computers to the front-end controllers. The same technique is used to verify the state-of-health of the safety computers and their interfaces to the CAMAC system.

Additionally, diagnostic information will be passed through the serial communication links connecting each front-end controller to the safety branch, allowing the safety computers to also pass judgment on the state-of-health of the front-end controllers. The process and safety computers will use this communication link to pass diagnostic data and MDAC configuration information to each other as an overall system check. This communications path will operate at a rate of 9600 baud and provide optical isolation between the process and safety branches.

2.3.4 Man-Machine Interface

The man-machine interface (MMI) serves as an interface between the system operators and the master data acquisition and control system. For discussion purposes the MMI has been separated into three discrete sections. These sections are identified as the Process MMI, the Safety MMI, and the Engineering Support Center MMI. The process and safety MMIs are two isolated sections of this subassembly of MDAC and are controlled by the computers in their respective branches. The Engineering Support Center's (ESC) MMI can be switched to either the process computer or the safety computer.

The two keyboards and two CRT monitors included in the Process MMI are mounted in the operator's console in the control room. The two keyboards permit the operators to input data, supervisory control commands, and requests for displays to the computer. The two CRTs are eight-color, high-resolution, 19-inch units used for viewing displays of TSTA operation and performance. One area of the CRT screen is dedicated to displaying alarm messages and informational messages to the operators.

This color graphics system features the selection of up to 256 alphanumeric, and graphic characters with individual control of two-character sizes and intensities, blink, reverse video, protect status, and color (one of eight). Two display generators serve as the interface between the process computers and the keyboard/CRT monitors. The display generators are dual ported, which allows the connection of both CPU-1 and CPU-2 to each unit for redundant operation. Both keyboard/CRT pairs can operate under the control of either CPU, or each CPU can control a single keyboard/CRT independently. In either configuration, the same or different displays can be obtained on the two CRTs simultaneously at the option of the operator.

The remaining equipment of this MMI consists of two logging printers that provide for sequential logs of alarms, supervisory control actions, and TSTA system performance. Each logging printer is dedicated to a particular process computer and may also be used as a plotter to copy CRT displays.

The safety system's MMI is essentially the same as that for the process system. It includes two keyboards and two 19-inch color CRTs, all mounted in the operator's console. The keyboards and CRTs are identical to those in the process system in order to reduce any operator errors associated with using a different control keyboard during an emergency situation. The displays and display format of the CRT are also the same as those of the process system.

The same commands that are used in the process branch will activate the same valves/processes when entered via the safety MMI keyboard. Again, the safety system will provide control of only those valves/processes/operating modes of TSTA deemed necessary for safe operation. The display generators of the safety system's MMI are dual ported to the LSI/11 safety computers, allowing for multi-redundant operation.

Two each plotter/printers will be used in the safety system for the purpose of logging alarms, supervisory control actions taken by the safety computers or input by way of the safety system's MMI keyboards, and an abbreviated list of system performance parameters.

Two each CRT/keyboards identical to those of the process and safety sections of the MMI will be placed in an outer office area of TSTA defined as the Engineering Support Center (ESC). These color displays will have no control capability; however, they will be able to select any of the displays available to the control room monitors. During normal operation, these displays will be used by the engineers and scientists to monitor TSTA operation and to evaluate the effect of any changes in the operating parameters being tested. These displays external to the control room will also be used for routine monitoring of conditions by the health physics staff.

Should an emergency ever occur, the ESC will then function as a center for evaluation and management of the emergency by the technical staff, leaving the control room free of unnecessary crowding and confusion. The intercom system will provide communications between the ESC and the control room.

TABLE 1
SUMMARY OF TSTA PARAMETERS

	DATA ACQUISITION		CONTROL	
	ANALOG CHANNELS	STATUS CHANNELS	ANALOG CHANNELS	DIGITAL CHANNELS
PROCESS BRANCH	525	871	23	806
SAFETY BRANCH	243	463	9	207
TOTAL	768	1,334	32	802

3. BIOGRAPHY

John J. Damran is a staff member in the Electronics Division at the Los Alamos National Laboratory, Los Alamos, New Mexico. He joined the Laboratory in April 1975 and has been primarily involved in the design and development of instrumentation and control systems. Prior experience includes 13 years of design and development of instrumentation, controls, and microelectronics. Mr. Damran received his B.S.E.E. degree at San Jose State University, San Jose, California. He is a Senior Member in the Instrument Society of America.

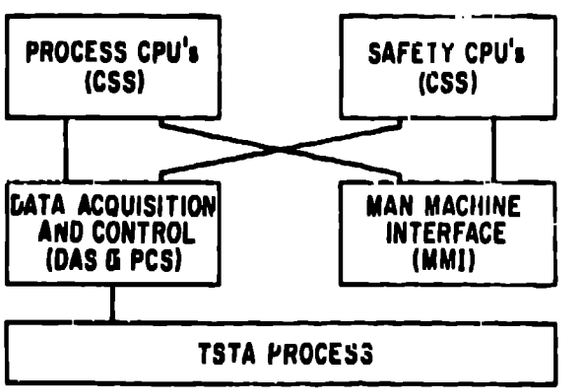

Figure 1
GENERAL BLOCK DIAGRAM OF MDAC

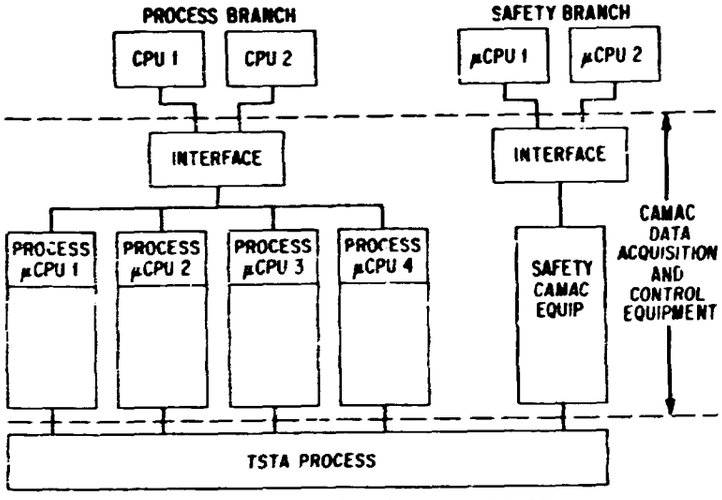

Figure 2 COMPUTERS' INTERFACES TO DATA ACQUISITION AND CONTROL SUBSYSTEMS

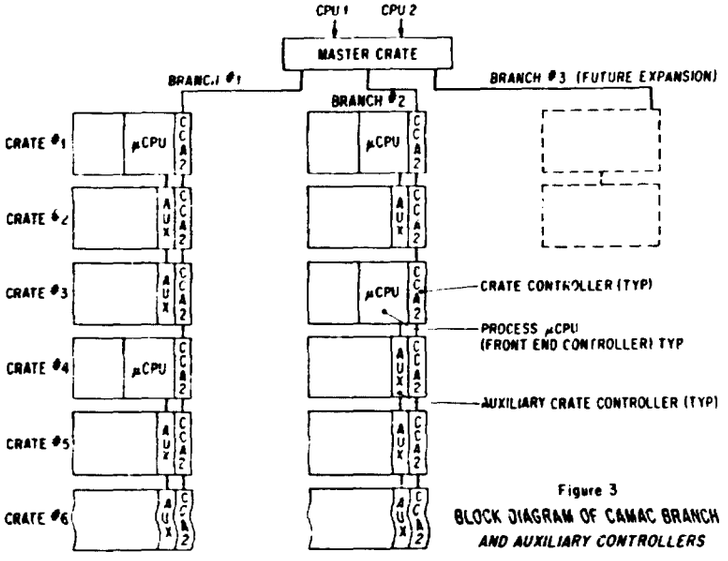

Figure 3 BLOCK DIAGRAM OF CAMAC BRANCH *AND AUXILIARY CONTROLLERS*

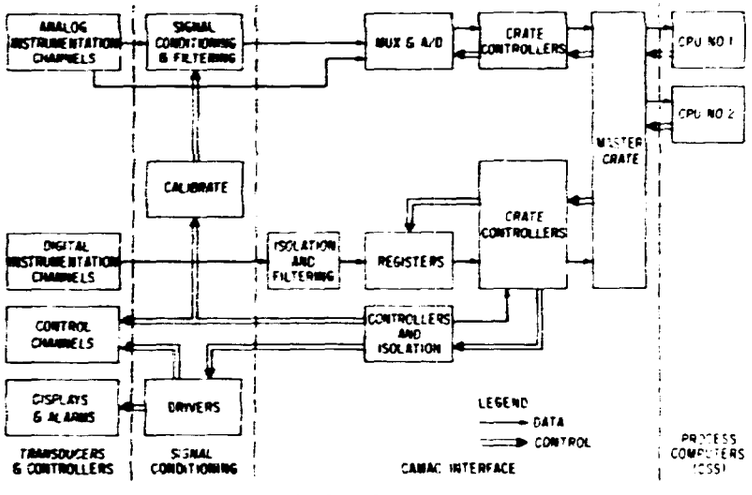

Figure 4 BLOCK DIAGRAM OF INTEGRATED DAS AND PCS

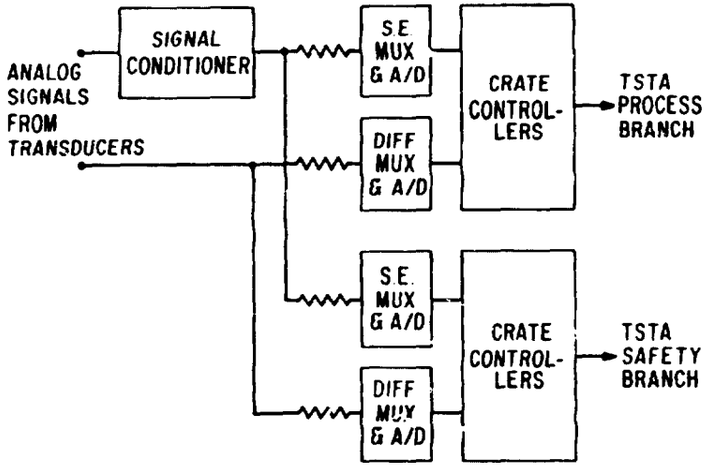

Figure 5 RESISTOR ISOLATION BETWEEN PROCESS AND SAFETY SYSTEMS FOR ANALOG SIGNALS

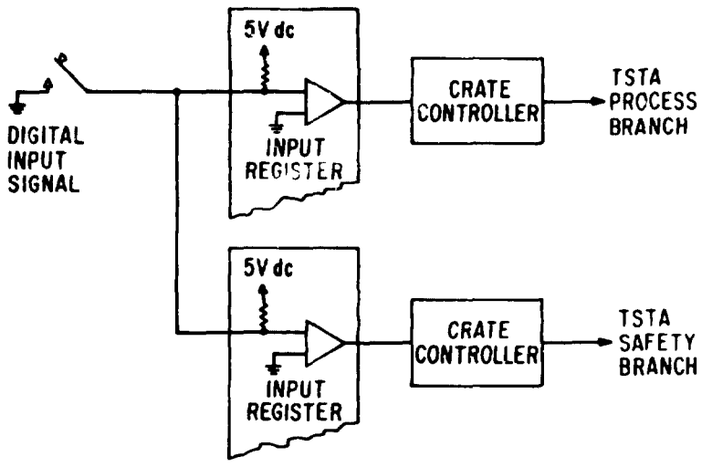

Figure 6 RESISTOR ISOLATION BETWEEN PROCESS AND SAFETY SYSTEMS FOR DIGITAL SIGNALS

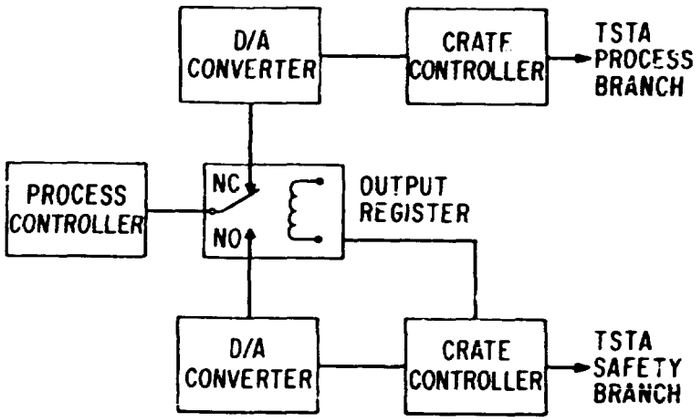

Figure 7
RELAY ISOLATION BETWEEN PROCESS AND SAFETY BRANCHED FOR ANALOG OUTPUT CONTROL SIGNALS

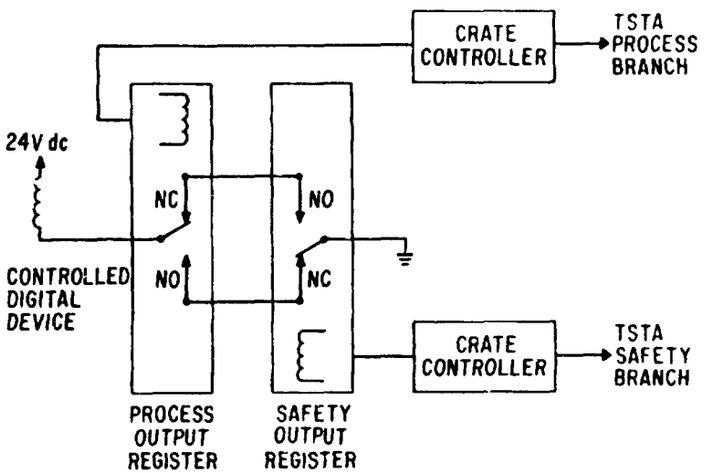

Figure 8 RELAY ISOLATION BETWEEN PROCESS AND SAFETY BRANCHES FOR DIGITAL OUTPUT SIGNALS

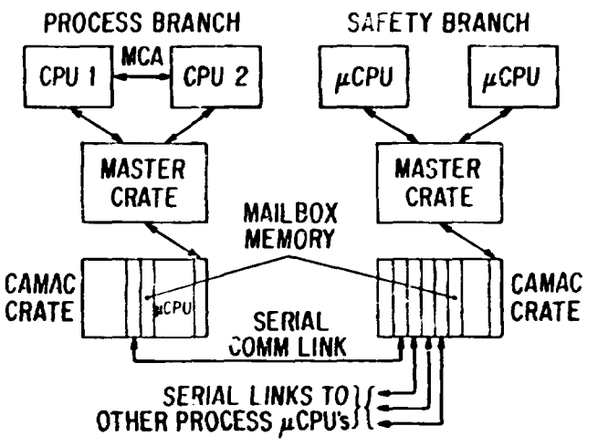

Figure 9
COMMUNICATION PATHS BETWEEN CPU's