



HEAVY MOVABLE
STRUCTURES, INC.

FIFTH BIENNIAL SYMPOSIUM

November 2nd - 4th, 1994

Holiday Inn Surfside
Clearwater Beach, Florida

SESSION WORKSHOP

PRESENTATIONS

"THE APPLICATION OF
TRIPLE MODULAR REDUNDANT (TMR)
PROGRAMMABLE LOGIC CONTROLS (PLC)
TO A HEAVY MOVABLE STRUCTURE"

by PHILLIP J. DIBB
The Oilgear Company

DISCLAIMER

It is the policy of the Corporation to provide a means for information interchange. It does not propagate, recommend or endorse any of the information interchanged as it relates to design principles, processes or products presented at the Symposium and/or contained herein. All Data are the authors' and not the Corporation's. Application of information interchanged is the responsibility of the user to validate and verify its integrity prior to use.

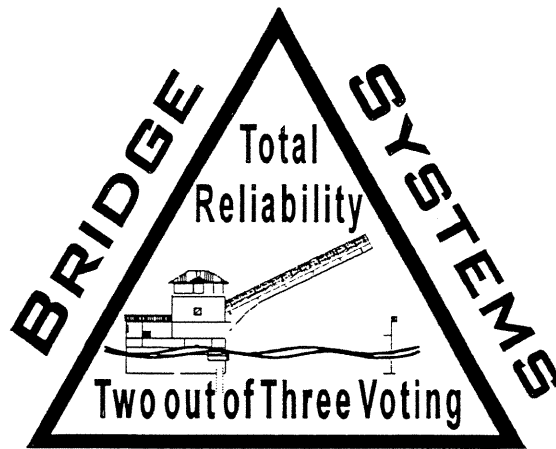
**THE APPLICATION OF
TRIPLE MODULAR REDUNDANT (TMR)
PROGRAMMABLE LOGIC CONTROLS (PLC)
TO A HEAVY MOVEABLE STRUCTURE**

By Phillip J. Dibb

of

*The Oilgear Company
Milwaukee, Wisconsin*

*Fifth Biannual Symposium
November 1994*



2 0 0 3

Oilgear **SERVO CONTROL PRODUCTS**

INTRODUCTION

Triple Modular Redundant (TMR) systems have achieved a solid reputation. Typical applications for TMR systems include: emergency shutdown, fire and gas detection systems, monitor and control of nuclear power plants, boiler/burner management, and batch processing systems for the petroleum and pharmaceutical industry. Past TMR systems were extremely specialized and quite expensive. However, in this era of rapidly expanding computer software and PLC technology, TMR systems are becoming more affordable and are being applied when reliability, safety, or environmental impact is present. The TMR system also includes comprehensive diagnostic reporting which greatly aids projects from installation/start-up and in future years of service.

PROTECTIVE SYSTEMS

Control system technology can be classified in three basic classifications:

- ▲ Fail Safe
- ▲ Dual Redundant
- ▲ Triple Modular Redundant (TMR)

Fail Safe

Fail Safe typically shuts down the process, even when the problem is a hardware component. Many times false trips result in considerable economic loss and sometimes a potentially hazardous process disturbance. Simple fail safe systems are many times plagued with false trips.

Dual Redundant

Many times, dual redundant designs involve the risk of an incorrect decision made between the primary and backup system, as well as creating a problem if the backup system does not function correctly.

Triple Modular Redundant (TMR)

The triple modular redundant control systems are typically stated to be 10 to 25 times more reliable than the dual redundant system and up to 50 times more reliable than non redundant system. Triple modular redundant systems tolerate failures of one or more components while continuing execution of the expected task. A TMR system can be utilized in any process requiring continuous operation and a high degree of safety. A TMR system allows for ease of maintenance ability by on site personnel. This phase is often times overlooked as part of the system design. A considerable amount of time and taxpayer money are invested into bridge control systems. The best way to receive daily dividends on this investment is to have the bridge system work successfully, every time.

THE TMR SYSTEM CONFIGURATION

TMR systems are accomplished with two configurations - either hardware or software.

Hardware: The hardware configuration requires customized IC's and circuit boards to utilize the inner connectability of the control circuits. This system has the benefit of being slightly higher speed but has the disadvantage of being customized hardware, available only through the supplier of that product.

Software: These systems are available again on custom hardware or utilizing conventional PLC hardware with a TMR software package running.

Both the hardware and software solutions offer a highly fault tolerant system. The typical TMR system includes three parallel independent channels of control to isolate a failed component through two out of three voting on the state of the inputs and outputs. Diagnostics are cross checked by all three processors, which avoids the fallacy of the self test employed in dual processor systems. A single input from the process is wired to input modules of three separate processors. Through triple redundant communication links, each processor transfers the sensed state of the input to the other two processors. An input voter in each processor provides the voted result for the application program. Input disagreements are reported so that the faulty input sensor or input module can be easily repaired. The output from each processor is routed to the load circuit which performs a two out of three vote to reject the data from any one failed processor or output module. The voting circuit incorporates output feedback so that the processors can monitor the output circuit for failures. Although there are three separate independent processors, the application program (ladder logic) is developed and downloaded as if the system was a single PLC. The replication of inputs, outputs, and processors is totally transparent to the application program. All redundancy is configured with a Windows based package integrated within the PLC programming package. Complete diagnostics is integrated into each processor, which monitors the operation of the other processors. I/O points are exercised for open and shorted circuits without disrupting the process. A Windows based fault history display reports any failures for maintenance action while the fault map can be employed to program a fault response on a per point basis.

Fault Tolerance

The TMR system is fully fault tolerant. That is, any single short or open I/O circuit, PLC fault, power supply fault, or other failure will not lead to a loss of control of the system.

Complete Diagnostics

The TMR system includes diagnostics as part of the core system. All inputs and outputs are exercised during each PLC scan for shorted and open circuits, faults are isolated and reported to the I/O point level. Testing is non intrusive to the user application program and I/O and is interrupted by I/O state changes even at full speed. Another unique feature is the ability to detect shorts between any two input circuits, which is a requirement for special safety systems.

On Line Repair

The TMR system features a modular replacement and repair philosophy. All modules can be replaced on line without disrupting the system or process.

SYSTEM HARDWARE OVERVIEW

Input Subsystem

The input to a TMR system can be a single or multiple devices. Figure 1 depicts a single device connected to three input channels, one located in each CPU.

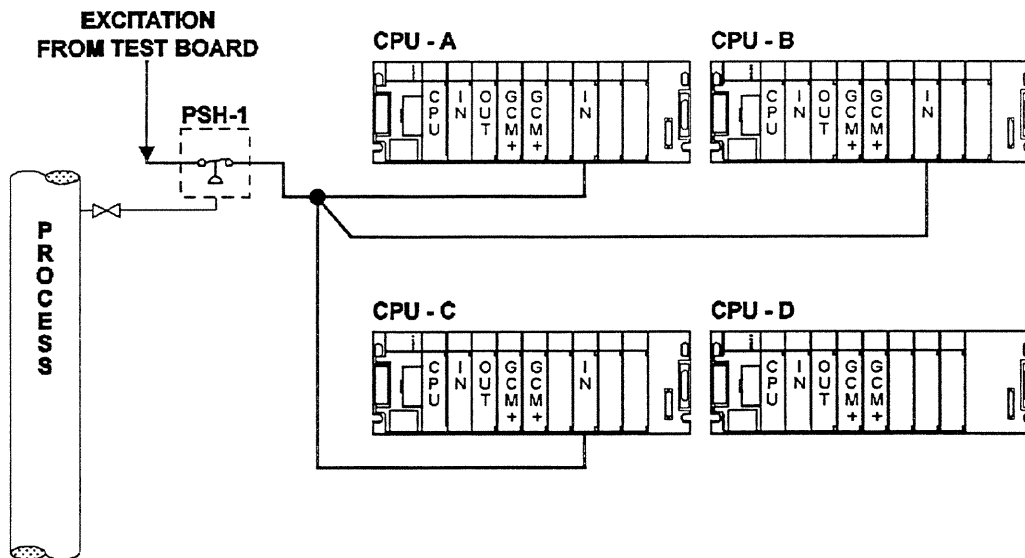


Figure 1: Single Input to TMR System

Each CPU reads the appropriate input; input data is compared to the other CPUs to determine the two out of three voting. The innovative diagnostics built into the TMR system are designed to uncover all hidden faults, such as short or open circuits. Short circuit detection includes scanning for shorts between two or more input circuits. The diagnostics are started and completed in the same PLC scan and are guaranteed to be non-intrusive to the user's application and output loads. The inputs are individually pulsed off to check for a "stuck on" condition. This is a "dangerous state" in traditional safety circuits, since the I/O's are normally energized. Each input field device is sourced from a PLC output. This allows for the testing action to be accomplished.

Figure 2 illustrates TMR system interconnection between the Central Processing Units, the input system diagnostics Test Board and the Input board. The Input Board is connected to the input devices that are mounted in the field. The Test board provides power to the input devices and interfaces diagnostic testing by the TMR system.

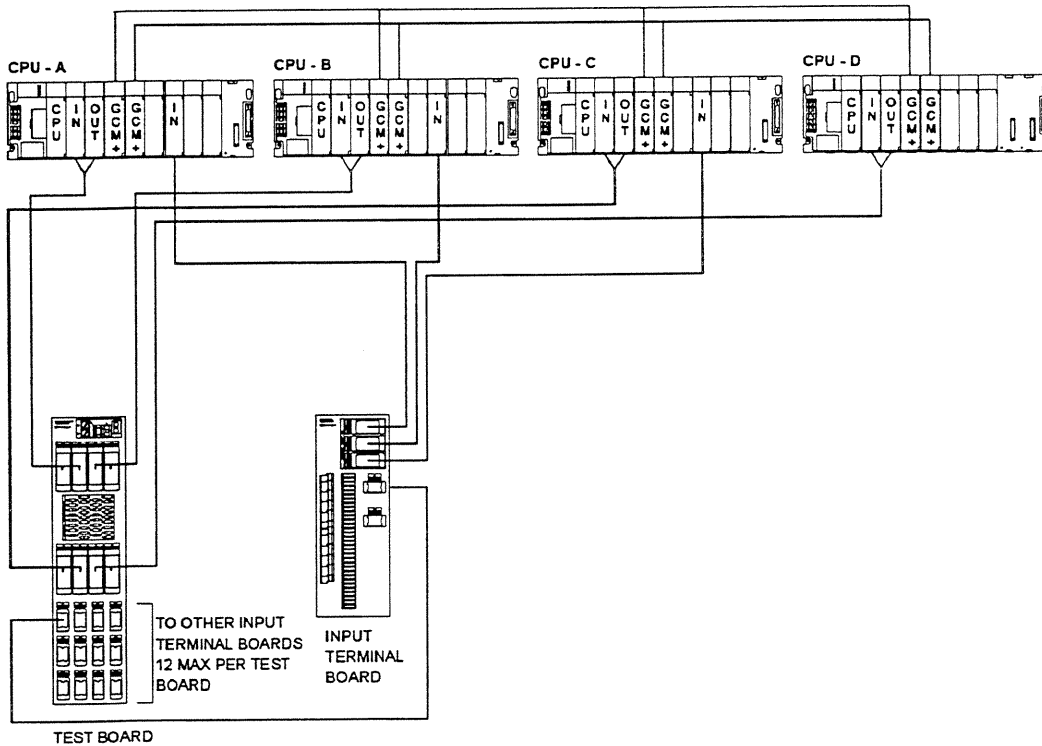


Figure 2: TMR Input System Block Diagram

Discrete field devices can also be used in duplex or triplex modes. Figure 3 demonstrates triplex mode operation. Triplex mode requires connection of three identical field devices to the same I/O point of each of the three TMR CPUs. (This varies from Figure 1, which showed one input device connected to the same I/O point of each of the three TMR CPUs.)

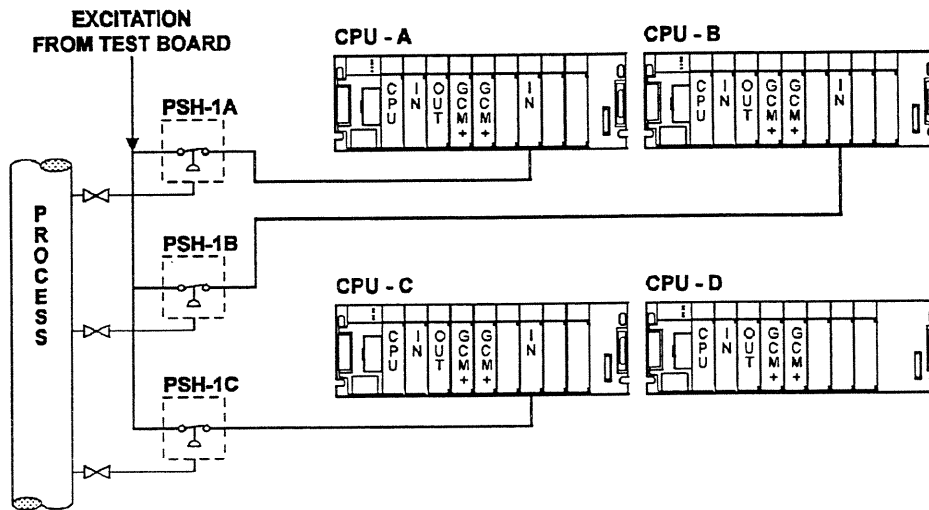


Figure 3: TMR Input-Triplex Mode

Figure 4 demonstrates duplex mode operation. Duplex mode requires connection of two identical field devices to the same I/O point of the first two of the three TMR CPUs.

NOTE: CPU A, CPU B and CPU C are the TMR Central Processing Units. CPU D provides output points that complete the H-pattern for an output. CPU D does not receive direct input information from the field, but does participate in the input voting process with information that is received through an inter CPU network.

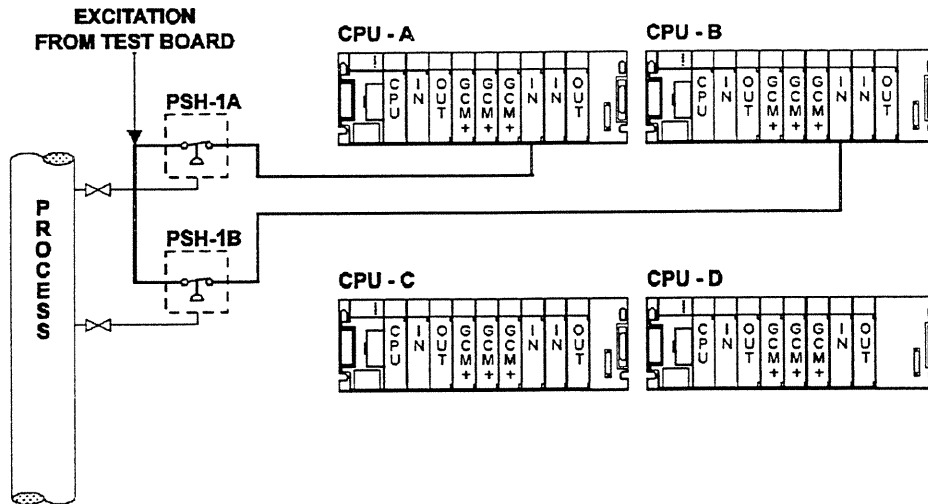


Figure 4: TMR Input-Duplex Mode

The Output Subsystem

Figure 5 illustrates TMR system interconnection between the Central Processing Units and the Output board. The Output Board is connected to the output devices that are mounted in the field. The Output board provides interfacing between the field device and the TMR system.

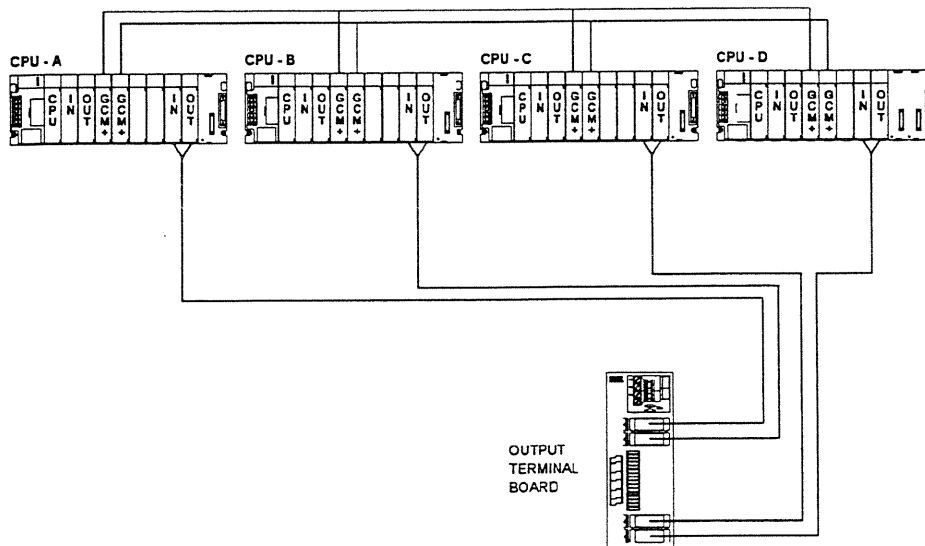


Figure 5: TMR Output System Block Diagram

The output device is connected to identical output points of CPU A, CPU B, CPU C and CPU D. CPU A and CPU B provide sourcing output points. CPU C and CPU D provide sinking output points. This output arrangement is called an H 4-output group.

The application logic passes data to a single location in the output image table for each load. The output table is transferred to the output module at the end of the CPU scan and then tested by the output voting circuitry. The voter circuit receives the three outputs from the PLC output modules. A fourth output, from the output module in the PLC D, generates the "AB" term and completes the two out of three vote. The fourth output represents the logical AND of the outputs of the first two processing units: CPU A and CPU B. The output vote is performed at the load when the four outputs are interconnected as shown in Figure 6. A feedback input from each of the four outputs is looped back into its respective PLC for integrity testing. The output vote is checked for discrepancies, which are logged in the fault history and fault map.

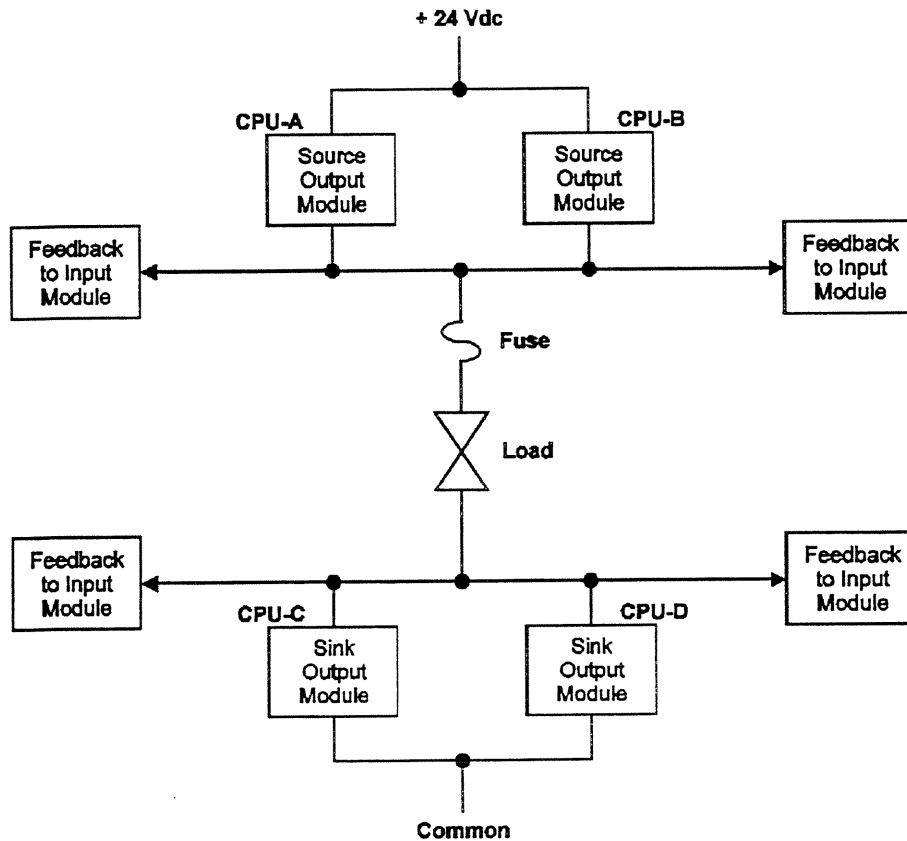


Figure 6: TMR H 4-Output Group

Each physical output is individually pulsed, both on and off for two milliseconds to verify that a stuck-off or stuck-on condition does not exist. This testing proceeds continuously, regardless of the commanded state of each load or the rate of the output load transitions. The testing cycle is completed about once every second. A more detailed layout of this H output voting circuit is pictured in Figure 6. This H circuit makes it impossible to have an error due to the failure of any one output module within the circuit.

Analog I/O

Analog inputs are handled in the same format as digital inputs. Analog outputs are also supported but in a slightly different manner.

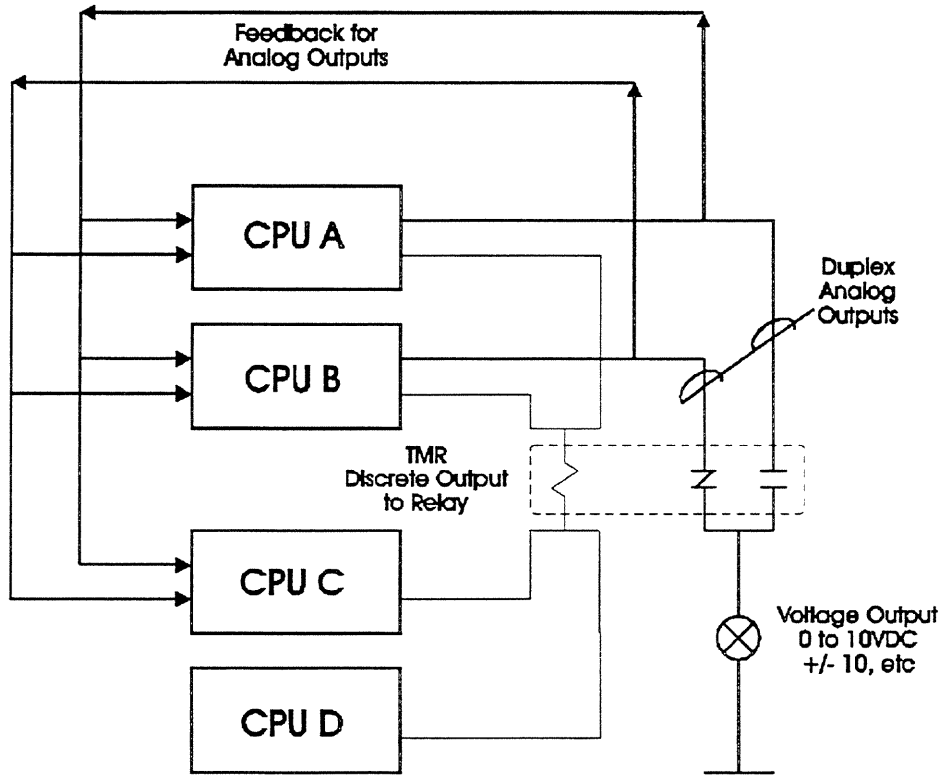


Figure 7: Redundant Analog Output Block Diagram

Analog outputs are handled as redundant. One output from CPU A or one output from CPU B is selected by the use of an external relay to drive the analog load. This relay is driven by a voted TMR discrete output. Each of the two analog outputs are feedback into CPU A and CPU C for diagnostic purposes. Figure 7 illustrates the basic elements of the analog subsystem.

DIAGNOSTICS

One of the most beneficial features within the TMR system is extensive diagnostics. TMR system diagnostics support maximum system uptime by greatly reducing system debug and maintenance troubleshooting time.

The TMR system can isolate and report I/O faults to the I/O point level. A fault map can be examined by the application program. The application program can initiate appropriate action upon report of an I/O failure

Input Diagnostics

Line Fault

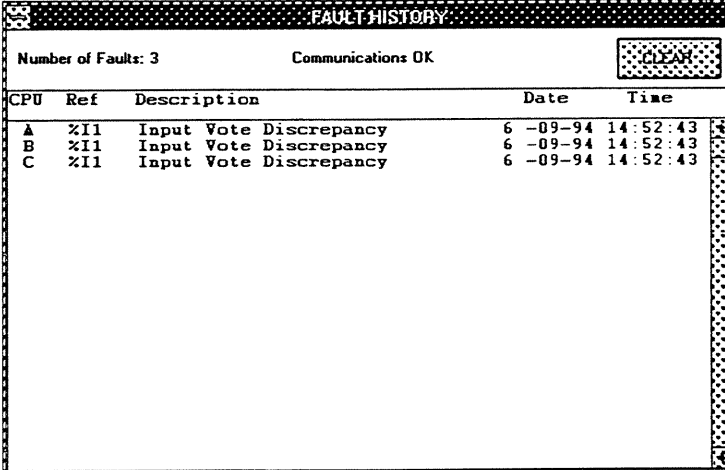
The TMR input can be configured for supervision of input wiring. A line fault will be reported when either a short or an open circuit fault of field wiring is detected. This will depend on the wiring configuration.

Diagnostics

Discrete inputs can be configured for short circuit testing. This tests the normally open inputs to determine if they can attain their off state and checks for cross connection of inputs.

Discrepancies

This diagnostic selection determines whether the raw inputs disagree with the voted result. If there is any discrepancy between the original input value and the input in its voted state, the PLC automatically places a message in the Fault History Table and sets a bit in the fault map. An example of this Fault History Table is shown below.



The screenshot shows a window titled "FAULT HISTORY". At the top left, it says "Number of Faults: 3" and "Communications OK". There is a "CLEAR" button in the top right corner. Below this is a table with the following data:

CPU	Ref	Description	Date	Time
A	Z11	Input Vote Discrepancy	6 -09-94	14:52:43
B	Z11	Input Vote Discrepancy	6 -09-94	14:52:43
C	Z11	Input Vote Discrepancy	6 -09-94	14:52:43

Figure 8: Input Discrepancy Report Screen

OUTPUT DIAGNOSTICS

No Load Fault

For voted output loads, individual outputs can be configured to enable or disable reporting of load monitoring faults.

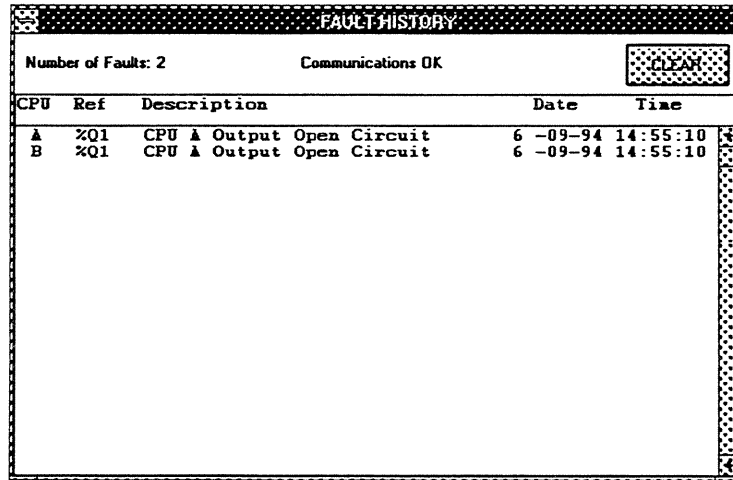
If the system load is less than 10 milliamps, load monitoring should be disabled.

Open/Shorted Circuitry Faults

The discrete TMR outputs can determine whether an individual output module is in a shorted or open circuited condition.

Output Discrepancy Reporting

Each output module in the TMR system is monitored. A report is made if the output module does not agree with the appropriate image table value. Below is an example of an output fault history report.



The screenshot shows a window titled "FAULT HISTORY". At the top left, it says "Number of Faults: 2". At the top right, it says "Communications OK" and there is a "CLEAR" button. Below this is a table with the following data:

CPU	Ref	Description	Date	Time
A	%Q1	CPU A Output Open Circuit	6 -09-94	14:55:10
B	%Q1	CPU A Output Open Circuit	6 -09-94	14:55:10

Figure 9: Output Discrepancy Report Screen

SUMMARY

The TMR system technique is cost effective, while providing continuous operation and a high degree of safety. Easy maintenance is another benefit of the system because of the high level of built-in diagnostics. The TMR system is transparent to the PLC programmer. Programs are entered and modified as if the system contained only one PLC. All processors are on-line together and any one system can be shut down for repair. There is no switch over or bump that is commonly experienced in the hot back-up PLC system. The TMR system is available in either custom or conventional hardware. It is recognized as the most fault tolerant PLC system available today.

ACKNOWLEDGMENTS

Trimation, Inc., Charlottesville, Virginia