1. Description

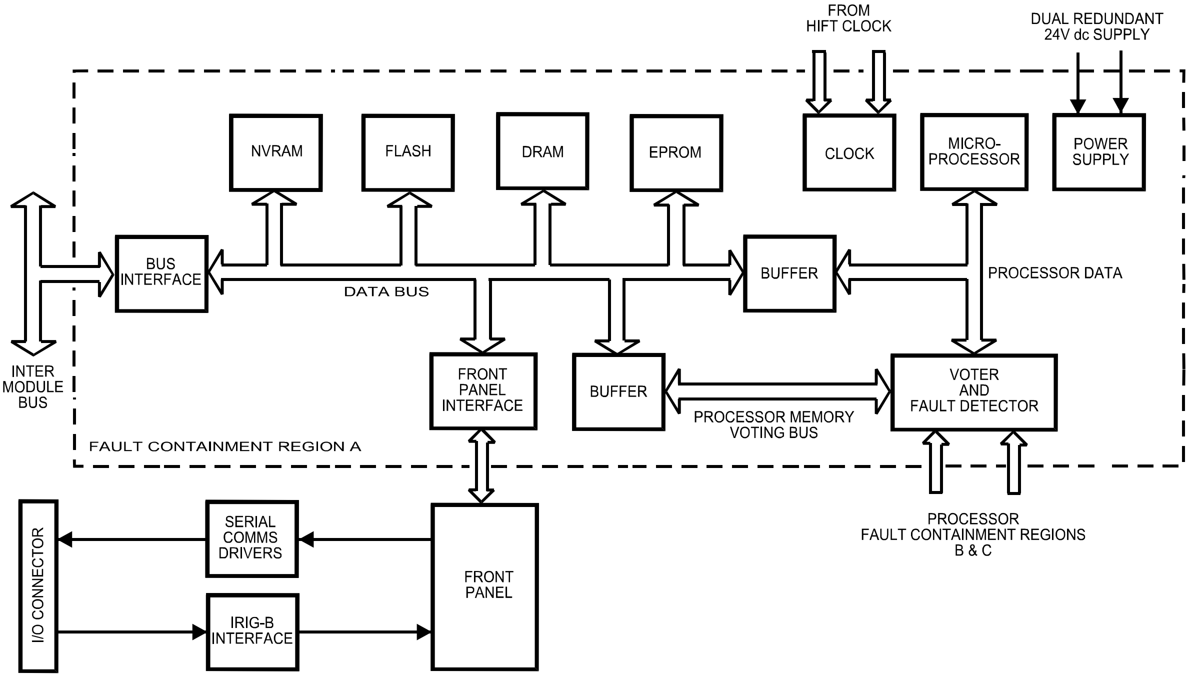

Figure 1 Module Architecture

1.1. Overview

The Trusted TMR Processor is a fault tolerant design based on a Triple Modular Redundant (TMR) architecture operating in a lock-step configuration. Figure 1 shows, in simplified terms, the basic structure of the Trusted TMR Processor module.

The module contains three Processor fault containment regions (FCR), each containing a Motorola Power PC series Processor and its associated memory (EPROM, DRAM, Flash ROM, and NVRAM), memory mapped I/O, voter and glue logic circuits. Each Processor FCR has voted two-out-of-three (2oo3) read access to the other two Processor's FCR memory systems to eliminate divergent operation.

The module's three Processors store and execute the application program, scan and update the I/O modules and detect system faults. Each Processor executes the application program independently, but in lock-step synchronisation with the other two. Should one of the Processors diverge, additional mechanisms allow the failed Processor to re-synchronise with the other two.

Each Processor has an interface which consists of an input voter, discrepancy detector logic, memory, and an output driver bus interface to the Inter-Module Bus. The output of each Processor is connected by the module connector to a different channel of the triplicated Inter-Module Bus.

Communication between the Trusted TMR Processor and modules in other chassis is via either a Trusted Interface module, such as the Trusted TMR Interface to a Regent+Plus I/O chassis, or an Expander Interface to an Expander chassis.

The functions of the four types of module memory are:

- **EPROM** - Holds module bootstrap loader
- **Flash ROM** - Stores module firmware and the application program
- **DRAM** - Working memory with scaleable capacity
- **NVRAM** - Holds data such as event logs and retained program data

Note: The NVRAM provides data retention for up to 10 years.

The Front Panel comprises a fault containment region (FCR D) separate from the other FCRs and contains non-critical functions. These include:

- The diagnostics port and maintenance enable keyswitch mounted on the front panel of the Processor.
- The serial communications drivers and the IRIG-B interface. These are accessed through the I/O connector via adapter units at the rear of the Processor.
- Participates in all module voting operations.
- Sends Fault/Fail signals to external indicators via the adapter units at the rear of the Processor.

Two IRIG-B input standards are available to the Processor; IRIG-B002 and IRIG-B122. The standard used by the Processor is controlled by software setting a flag in the memory. The IRIG-B signals are used to synchronise systems and time-stamp entries in the Sequence of Events (SOE) log.

Three serial communication options are available from the 4-channel Universal Asynchronous Receiver/Transmitter (UART). These are detailed as follows:

Channel 0	Front Panel Diagnostic Port (RS232)
Channel 1	Not configured
Channel 2	Communications Serial Port 2 (RS422/485)
Channel 3	Communications Serial Port 3 (RS422/485)

The Trusted operating system (Trusted OS) is used in support of the Motorola Power PC series processor architecture. The real time kernel is a high speed, high functionality kernel made for fault tolerant distributed systems. The distributed communication is made transparent over all processors.

The kernel provides basic services (such as basic memory management), and interference free software environments which allow software of various integrity levels to reside and co-operate in a single processing environment.

An Application Program Interface (API) provides a consistent run-time interface for the services provided by the Trusted TMR Processor to the application program. The API also performs the same function to system-specific software executing within the Trusted TMR Processor.

1.2. Hardware Implemented Fault Tolerant (HIFT) Clock

Each of the Processor and Front Panel FCR regions has its own HIFT clock, which are provided with a synchronisation reference signal from the fault tolerant reference clocks.

1.3. Power Distribution

Each of the Processor and FCRs derive their internal voltages from dual redundant +24 Vdc power supplied via the module connector from the Trusted Controller chassis backplane.

1.4. Fault/Fail Relays

Each Processor generates a Fault and Fail signal from two relays located in the Front Panel IRIG containment region.

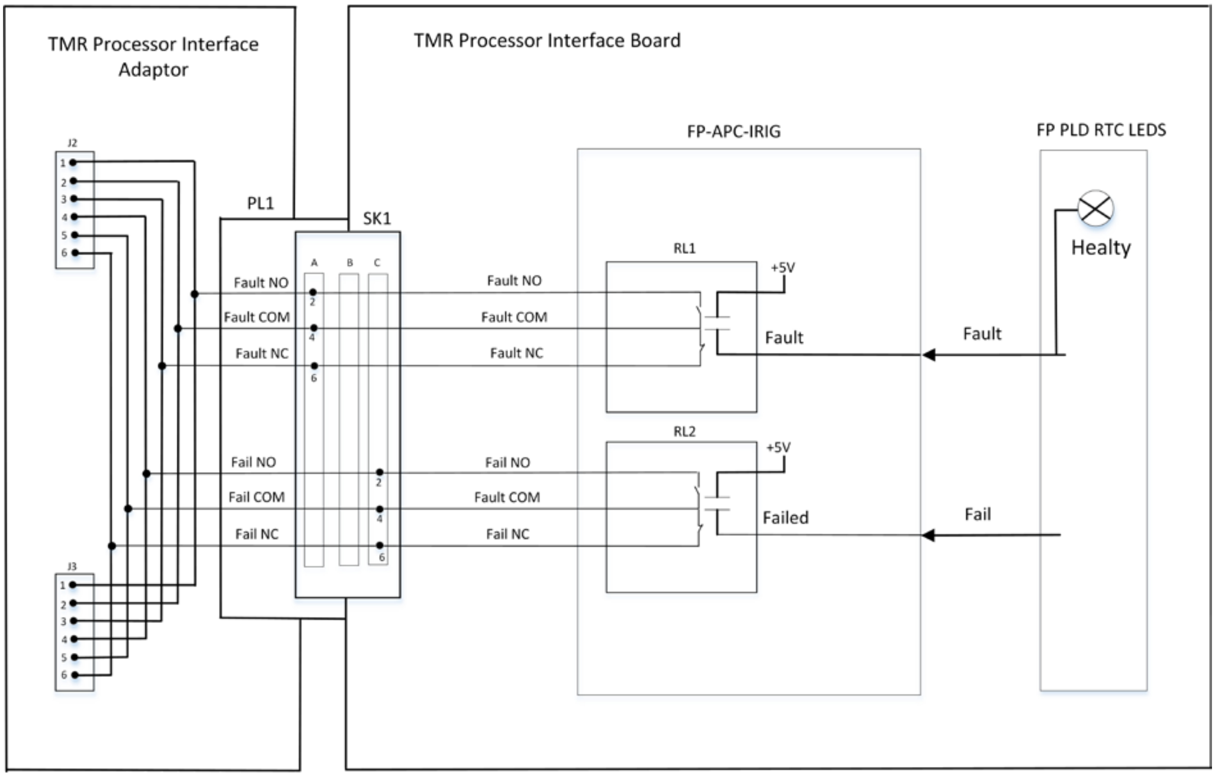

Figure 2 Fault/Fail Relays

The Fault and Fail signals are initiated by the Front Panel Light Emitting Diode (LED) containment region. A Fault signal is generated when a system fault occurs. The System Healthy LED flashes Red and the Fault signal drives the relay RL1 NC contacts open.

The Fail relay stays healthy if one of two Processors goes faulty and loses one slice but the other Processor takes over and goes active. If neither Processor is active with two working slices a Fail signal is generated indicating that the system has shut down. The Fail signal drives relay RL2 NC contacts open.

The Fail and Fault relay NC contact signals are routed through SK1 to the TMR Processor Interface Adapter to connectors J2 and J3.