Trusted TMR Processor

Product Overview

The Trusted® Processor is the main processing component in a Trusted System. It is a powerful, user-configurable module providing overall system control and monitoring facilities and processes input and output data received from a variety of analogue and digital Input / Output (I/O) modules across the Trusted TMR Inter-Module Communications Bus.

Features:

- Triple Modular Redundant (TMR), fault tolerant (3-2-0) operation.
- Hardware Implemented Fault Tolerant (HIFT) architecture.
- Dedicated hardware and software test regimes which provide very fast fault recognition and response times.
- Automatic fault handling without nuisance alarming.
- Time-stamped fault historian.
- Hot replacement (no need to re-load programs).
- IEC 61131-3 programming languages.
- Front panel indicators that show module status.
- Front panel RS232 serial diagnostics port for system monitoring, configuration and programming.
- IRIG-B002 and B122 time synchronisation signals.
- Active and Standby processor fault and failure contacts.
- Two RS422 / 485 configurable 2 or 4 wire connections.
- One RS485 2 wire connection.
- Certified to IEC 61508 SIL 3.

1. Description

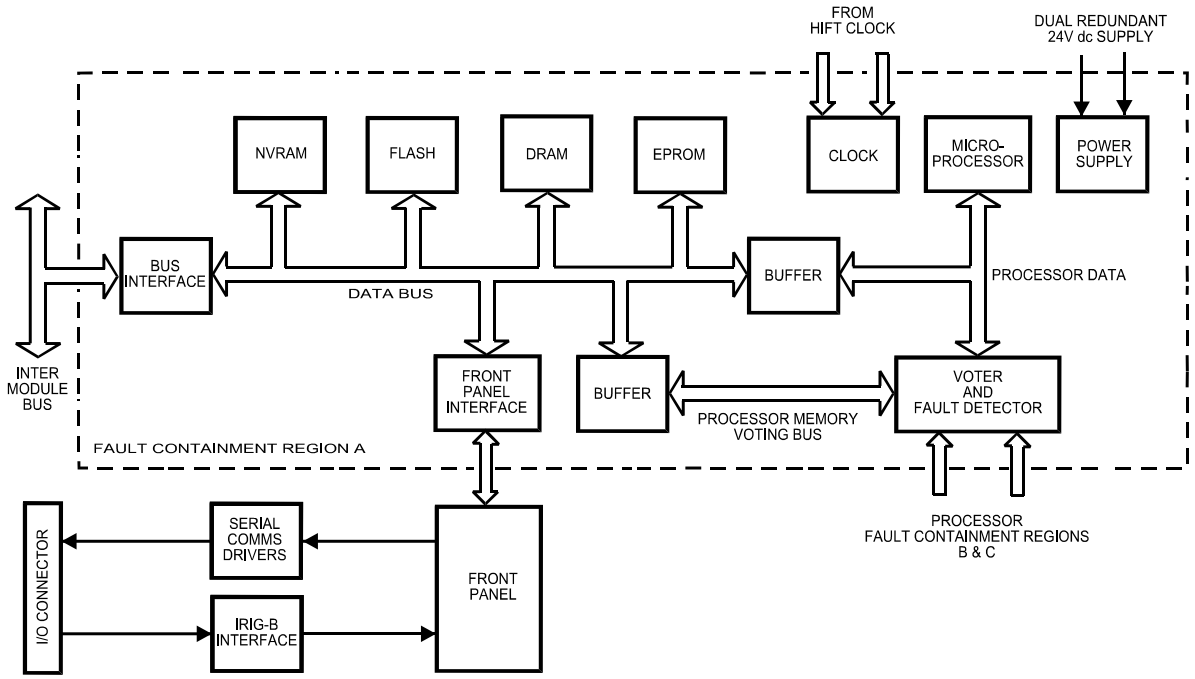

Figure 1 Module Architecture

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 NXP PowerQUICC® II™ series Processor and its associated memory (EPROM, DRAM, Flash ROM, and Flash RAM), 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.

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 (this is embedded in an FPGA)
- **Flash ROM** - Stores module firmware and the application program
- **DRAM** - Working memory with scaleable capacity
- **Flash RAM** - Holds data such as event logs and retained program data

The Front Panel contains a fault containment region (FCR D) separate from the other FCRs. It participates in the module voting operations. In addition it performs the following non-critical functions:

- 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 a T812X adapter unit at the rear of the Processor.
- 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 embedded 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 NXP PowerQUICC® II™ 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

A redundant fault tolerant clock circuit is used to provide the system clock signals to all FCRs.

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. The relays are both normally energised in a healthy system. For each relay, the normally open (NO) contact and normally closed (NC) contact together with their common (COM) are made available.

6. Specifications

Backplane (IMB) Supply	20 Vdc to 32 Vdc
Field Supply	N/A
Power Dissipation	30 W
Module Location	T8100 Processor Slot
Isolation: Module Supply, Module to Diagnostic Serial Port Module to: Rear Serial Ports, IRIG Ports & Relay Ports Between: Rear Serial Ports, IRIG Ports & Relay Ports	 50 V Basic (Continuous) {1} [Type tested at 1411 Vdc for 60 s]. 50 V Reinforced (Continuous) {1} 250 V Basic (Fault) {2} [Type tested at 2436 Vdc for 60 s]. 50 V Reinforced (Continuous) {1} 250 V Basic (Fault) {2} [Type tested at 2436 Vdc for 60 s].
Fusing	Not User Serviceable
Ports	3 Rear Serial Ports, RS-422/485 1 Diagnostics Serial Port, RS-232 1 IRIG-B002 1 IRIG-B122 1 Fault Relay, 0.5 A @ 24 Vdc 1 Fail Relay, 0.5 A @ 24 Vdc
Baud Rates	9600 baud to 115200 baud.
Communications Protocols (via Rear Serial Ports, see 3.1.8)	Modbus RTU
Real Time Clock: Clock retention time with module powered off.	8 hours {3}

Retained Variable Storage	4 KB total 1 byte per Boolean 4 bytes per Analogue 5 bytes per Timer
Maximum Application Size	960 KB {4}
SOE Buffer	1000 events
Operating Temperature	0 °C to 60 °C (+32 °F to +140 °F)
Storage Temperature	-25 °C to 70 °C (-13 °F to +158 °F)
Relative Humidity - Operating and Storage	10 % – 95 %, non-condensing
Environmental Specifications	Refer to Document 552517
Dimensions	
Height	266 mm (10.5 in)
Width	93 mm (3.6 in)
Depth	303 mm (12.0 in)
Weight	1.89 kg (4.17 lb)

Note 1) 50 Vrms Secondary circuit derived from Mains, OVC II up to 300V.

Note 2) 250 Vrms Mains circuit, OVC II up to 300V. Exposure to voltages at these levels shall be temporally constrained consistent with the system MTTR.

Note 3): RTC backup is by capacitor energy storage. Maximum charge time is 13 hours from fully discharged. Retention time takes capacitor aging into account.

Note 4): Applications larger than 860 KB may not allow handover from an active T8111 to a standby T8110B.