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 a Trusted TMR Inter-Module Communications Bus.

The range of applications for the Trusted TMR Processor vary in integrity level and include fire and gas control, emergency shutdown, monitoring and control, and turbine control.

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).
- Full suite of IEC 61131-3 programming languages.
- Front panel indicators that show module health and status.
- Front panel RS232 serial diagnostics port for system monitoring, configuration and programming.
- IRIG-B002 and 122 time synchronisation signals (available on T8110B only).
- Active and Standby processor fault and failure contacts.
- Two RS422 / 485 configurable 2 or 4 wire connections (available on T8110B only).
- One RS485 2 wire connection (available on T8110B only).
- TüV Certified IEC 61508 SIL 3.

Page intentionally left blank

PREFACE

In no event will Rockwell Automation be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment. The examples given in this manual are included solely for illustrative purposes. Because of the many variables and requirements related to any particular installation, Rockwell Automation does not assume responsibility or reliability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, with respect to use of information, circuits, equipment, or software described in this manual.

All trademarks are acknowledged.

DISCLAIMER

It is not intended that the information in this publication covers every possible detail about the construction, operation, or maintenance of a control system installation. You should also refer to your own local (or supplied) system safety manual, installation and operator/maintenance manuals.

REVISION AND UPDATING POLICY

This document is based on information available at the time of its publication. The document contents are subject to change from time to time. The latest versions of the manuals are available at the Rockwell Automation Literature Library under "Product Information" information "Critical Process Control & Safety Systems".

TRUSTED RELEASE

This technical manual applies to **Trusted Release: 3.6.1**.

LATEST PRODUCT INFORMATION

For the latest information about this product review the Product Notifications and Technical Notes issued by technical support. Product Notifications and product support are available at the Rockwell Automation Support Centre at
http://rockwellautomation.custhelp.com

At the Search Knowledgebase tab select the option "By Product" then scroll down and select the Trusted product.

Some of the Answer ID’s in the Knowledge Base require a TechConnect Support Contract. For more information about TechConnect Support Contract Access Level and Features please click on the following link:

https://rockwellautomation.custhelp.com/app/answers/detail/a_id/50871

This will get you to the login page where you must enter your login details.

IMPORTANT	A login is required to access the link. If you do not have an account then you can create one using the "Sign Up" link at the top right of the web page.

DOCUMENTATION FEEDBACK

Your comments help us to write better user documentation. If you discover an error, or have a suggestion on how to make this publication better, send your comment to our technical support group at http://rockwellautomation.custhelp.com

SCOPE

This manual specifies the maintenance requirements and describes the procedures to assist troubleshooting and maintenance of a Trusted system.

WHO SHOULD USE THIS MANUAL

This manual is for plant maintenance personnel who are experienced in the operation and maintenance of electronic equipment and are trained to work with safety systems.

SYMBOLS

In this manual we will use these notices to tell you about safety considerations.

⚡	SHOCK HAZARD: Identifies an electrical shock hazard. If a warning label is fitted, it can be on or inside the equipment.
⚠	WARNING: Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which can cause injury or death, property damage or economic loss.
⚠	ATTENTION: Identifies information about practices or circumstances that can cause injury or death.
⚠	CAUTION: Identifies information about practices or circumstances that can cause property damage or economic loss.
♨	BURN HAZARD: Identifies where a surface can reach dangerous temperatures. If a warning label is fitted, it can be on or inside the equipment.
❗	This symbol identifies items which must be thought about and put in place when designing and assembling a Trusted controller for use in a Safety Instrumented Function (SIF). It appears extensively in the Trusted Safety Manual.
IMPORTANT	Identifies information that is critical for successful application and understanding of the product.
NOTE	Provides key information about the product or service.
TIP	Tips give helpful information about using or setting up the equipment.

WARNINGS AND CAUTIONS

WARNING: EXPLOSION RISK

Do not connect or disconnect equipment while the circuit is live or unless the area is known to be free of ignitable concentrations or equivalent

AVERTISSEMENT - RISQUE D'EXPLOSION

Ne pas connecter ou déconnecter l'équipement alors qu'il est sous tension, sauf si l'environnement est exempt de concentrations inflammables ou équivalente

MAINTENANCE

Maintenance must be carried out only by qualified personnel. Failure to follow these instructions may result in personal injury.

CAUTION: RADIO FREQUENCY INTERFERENCE

Most electronic equipment is influenced by Radio Frequency Interference. Caution should be exercised with regard to the use of portable communications equipment around such equipment. Signs should be posted in the vicinity of the equipment cautioning against the use of portable communications equipment.

CAUTION:

The module PCBs contains static sensitive components. Static handling precautions must be observed. DO NOT touch exposed connector pins or attempt to dismantle a module.

ISSUE RECORD

Issue	Date	Comments
11	Oct 05	Format
12	Aug 06	Corrections
13	Sep 06	3.5 Scan Time Calc
14	Nov 06	Specifications
15	Dec 06	I/O Definition
16	Mar 07	Hot Swap
17	Sep 07	Max Scan Time
18	Feb 08	TTMRP_0 scaling
19	Sep 14	Fault/Fail Relay information added. Note added to OEM parameters Rack 1.
20	Sep 15	Rebranded and reformatted
21	Apr 16	Updated to incorporate IEEE standards with correction of typographical errors.
22	Jun 16	Standardise the Relative Humidity and Operating Temperature specifications

Page intentionally left blank

Table of Contents

1. Description

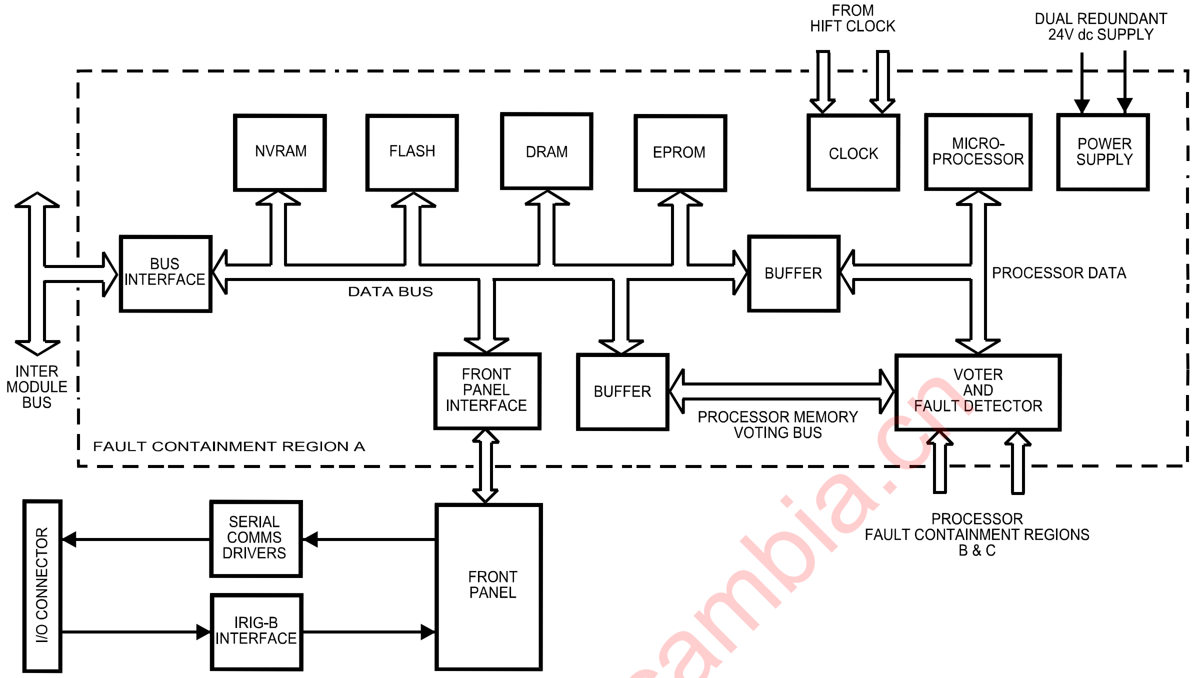

Figure 1 Module Architecture

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.

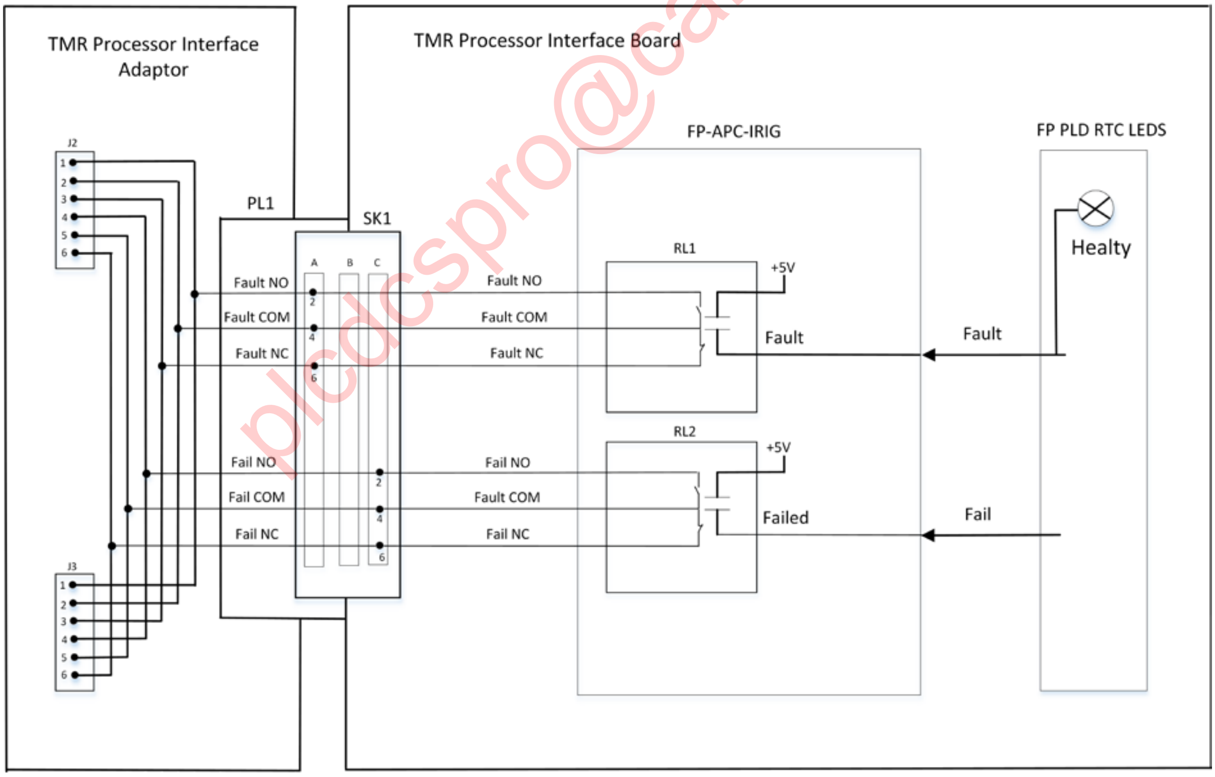

Figure 2 Fault/Fail Relays

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.

2. Installation

2.1. Module Insertion/Removal

CAUTION:

The module contains static sensitive parts. Static handling precautions must be observed. Specifically ensure that exposed connector pins are not touched. Under no circumstances should the module housing be removed.

Before installation, visually inspect the module for damage. Ensure that the module housing appears undamaged and inspect the I/O connector at the back of the module for bent pins. If the module appears damaged or any pins are bent, do not install the module. Do not try to straighten bent pins. Return the module for replacement.

Ensure that the module is of the correct type.

Record the module type, revision and serial number before installation.

To install the module:

1. Ensure that the field cable assembly is installed and correctly located.
2. Release the ejector tabs on the module using the release key. Ensure that the ejector tabs are fully open.
3. Holding the ejectors, carefully insert the module into the intended slot.
4. As soon as the Front Panel LEDs illuminate, push the module fully home by pressing on the top and bottom of the module fascia. The module should be inserted promptly to ensure that it connects to the Interface Adapter before reading the licenses.
5. Close the module ejectors, ensuring that they click into their locked position.

The module should mount into the chassis with a minimum of resistance. If the module does not mount easily, do not force it. Remove the module and check it for bent or damaged pins. If the pins have not been damaged, try reinstalling the module.

2.2. PCBs and Connectors

The Trusted TMR Processor comprises five separate Printed Circuit Board (PCB) assemblies:

1. Three identical Processor boards.
2. One Riser board to provide the connections between the PCB assemblies.
3. One module Main board that provides the inter-module bus connection and Front Panel facilities.

2.3. Module Pinout Connections

2.3.1. External I/O Connector (PL1)

This connector provides a number of discrete input and outputs. These are provided to allow the Trusted TMR Processor status to be monitored by external hardware, and to allow the Trusted TMR Processor to monitor the power supply status signals. The connector also provides access to the communications ports and connections for IRIG-B input signals. To enable the communications ports and IRIG-B facilities to be accessed, the user must install the following:

- Processor Interface Adapter T8120 for the communications ports.
- Processor Interface Adapter Unit (IRIG-B) T8121 for both communications ports and IRIG-B facilities.

Note: IRIG-B and serial facilities are only available on the T8110B

PL1 is a 48-way DIN41612 E type connector.

	Row		
Pin	A	C	E
2	Fault relay (NC)	DIAG_RTN	Failed relay (NC)
4	Fault relay (common)	DIAG_IN_1	Failed relay (common)
6	Fault relay (NO)	0 V Port 1	Failed relay (NO)
8	Not Connected	Serial Port 1 B	Not Connected
10	5V_D	Serial Port 1 A	IRIG-B122+
12	DATA_OUT	0V Port 2	IRIG-B122-
14	ENABLE	Serial Port 2 B TX	Reserved
16	DATA_IN	Serial Port 2 A TX	Reserved
18	CLK	Serial Port 2 B RX/TX	IRIG-B002-
20	0 V	Serial Port 2 A RX/TX	IRIG-B002+
22	Chassis GND	0 V Port 3	Chassis GND
24	Chassis GND	Serial Port 3 B TX	Chassis GND
26	Chassis GND	Serial Port 3 A TX	Chassis GND

	Row		
Pin	**A**	**C**	**E**
28	24 V PSU 1 LV Warning	Serial Port 3 B RX/TX	24V PSU 1 Fail Shutdown
30	24 V PSU 2 LV Warning	Serial Port 3 A RX/TX	24V PSU 2 Fail Shutdown
32	24 V Return	24 V Return	24V Return

Table 1 External I/O Connector Pin-out

Page intentionally left blank

3. Application

3.1. Module Configuration

The Trusted TMR Processor requires no hardware configuration.

Every Trusted System requires a System.INI configuration file. Details of how to design this are given in PD-T8082 (Trusted Toolset Suite). The configuration has a Processor assigned to the left slot of the Processor chassis by default. The System Configurator allows the selection of options on ports, IRIG and system functions. The use of the System Configurator is described in PD-T8082. The options are described below.

3.1.1. Updater Section

If Auto Protect Network Variables is selected, this configures the Trusted System to use a reduced Modbus Protocol map. See product description PD-8151B (Trusted Communication Interface Module) for further details.

Inter Group Delay equates to the Modbus update cycle. This is the minimum period between successive Modbus update messages sent to each of the Communications Interface Modules. The default value (as shown) is 50 ms which provides a compromise between latency and performance. Adjustment is made in 32 integer ms increments, i.e. a value of 33 will equal 64 ms as will 64.This may be increased or decreased as required, however since only one update message is sent per application scan, and an application scan may often be more than 50 ms, there is little benefit in adjusting this variable.

3.1.2. Security Section

The above display is also used to configure a password allowing the user to interrogate a Trusted System using the Windows-based HyperTerminal facility or a similar terminal program. The password is configured by selecting the New Password button and entering the new password twice in the displayed dialogue box.

3.1.3. ICS2000 Section

This section only applies to Trusted Systems connected via a Trusted to ICS2000 Interface Adapter to an ICS2000 system. This allows the data sources for the three mimic tables to be selected. Please refer to your Trusted supplier for further information.

3.1.4. System Section

WARNING:

Changes made to the System section may affect System performance, Fault Detection times and violate the process safety tolerances.

Entries to this section are typed directly into the SYSTEM Section text window.

DEFINITIONS

- **NIO Module** - Native Input or Output (I/O) Module. This refers to all I/O modules resident in a Trusted Chassis. It does not refer to I/O modules resident in other chassis types and communicating via a bridge interface module.
- **Dual I/O** - Module using two voted circuits to connect to a field device.
- **TMR I/O** - Module using three voted circuits to connect to a field device.

rim_interval

The value is specified in milliseconds. It specifies the minimum amount of time that must elapse between polls of Trusted TMR Interface Modules.

Changes to this value are reflected by the system immediately after the System.INI file is loaded.

Format:

- rim_interval=xx
- Default is 0.

pim_interval

The value is specified in milliseconds. It specifies the minimum amount of time that must elapse between polls of the Trusted Communication Interface Modules.

Changes to this value are reflected by the system immediately after the System.INI file is loaded.

Format:

- pim_interval=xx
- Default is 0.

discrepancy_val

The value is specified in milliseconds. It specifies the time that a TMR input or output channel must be discrepant before the TMR Processor reports the Channel Discrepancy fault.

The value applied here will affect all TMR NIO Modules (not Dual NIO Modules).

Changes to this value are not implemented until the TMR Processor is rebooted after the download of the System.INI file.

Format:

- discrepancy_val=xx
- Default is 2000.

dual_discrepancy_val

The value is specified in milliseconds. It specifies the time that a Dual input or output channel must be discrepant before the TMR Processor reports the Channel Discrepancy fault.

The value applied here will affect all Dual NIO Modules.

Changes to this value are not implemented until the TMR Processor is rebooted after the download of the System.INI file.

Format:

- dual_discrepancy_val=xx
- Default is 2000.

ana_discrep_val

The value is specified as 512 counts per volt. It specifies the allowed difference between voltage readings of Analogue Input channel slices before the TMR Processor indicates a Channel Discrepancy.

The value applied here affects all Analogue Input Modules (Dual and TMR).

Changes to this value are not implemented until the TMR Processor is rebooted after the download of the System.INI file.

Format:

- ana_discrep_val=xx
- Default = 40 (40/512 volts or 78 mV).

dig_discrep_val

The value is specified as 512 counts per volt for T8402 and T8403 and 128 counts per volt for T8423. It specifies the allowed difference between voltage readings of T8402, T8403 and T8423 Digital Input channel slices before the TMR Processor indicates a Channel Discrepancy.

Changes to this value are not implemented until the TMR Processor is rebooted after the download of the System.INI file.

Format:

- dig_discrep_val=xx
- Default = 250 (e.g. 250/512 volts or 512 mV for T8403).

di120vac_discrep_val

The value is specified as 100 counts per volt. It specifies the allowed difference between voltage readings of T8424 Digital Input channel slices before the TMR Processor indicates a Channel Discrepancy.

Changes to this value are not implemented until the TMR Processor is rebooted after the download of the System.INI file.

Format:

- di120vac_discrep_val=xx
- Default = 500 (500/100 volts or 5 V).

do_discrep_val

The value is specified in counts per volt and matches the module voltage reading scale. It specifies the allowed difference between voltage readings of Digital Output channel slices before the TMR Processor indicates a Channel Discrepancy. This setting is used in all Digital Output Modules and T8449.

Changes to this value are not implemented until the TMR Processor is rebooted after the download of the System.INI file.

Format:

- do_discrep_val=xx
- Default = 1000 (e.g. 1000/500th volts or 2 V for T8451).

ao_discrep_val

The value is specified as 500 counts per volt. It specifies the allowed difference between voltage readings of Analogue Output channel slices before the TMR Processor indicates a Channel Discrepancy.

This applies to T8480 analogue output modules only.

Changes to this value are not implemented until the TMR Processor is rebooted after the download of the System.INI file.

Format:

- ao_discrep_val=xx
- Default = 250 (250/500 volts or 500 mV).

zim_discrep_val

The value is specified as 500 counts per volt. It specifies the allowed difference between voltage readings of Zone Interface Module inputs before the TMR Processor indicates a Channel Discrepancy.

This applies to T8448 ZIM Modules (input channels only).

Changes to this value are not implemented until the TMR Processor is rebooted after the download of the System.INI file.

Format:

- zim_discrep_val=xx
- Default = 200 (200/500 volts or 400 mV).

smm_discrep_val

The value is specified as rpm. It specifies the allowed difference between rpm measurements on a T8442 Speed Input channel set before the TMR Processor indicates a Channel Discrepancy.

This applies to T8442 Speed Monitor Modules (input channels only).

Changes to this value are not implemented until the TMR Processor is rebooted after the download of the System.INI file.

Format:

- smm_discrep_val=xx
- Default = 10 rpm.

Note: That there is no discrepancy checking on a T8444.

3.1.5. ISaGraf Configuration Section

IsaGraf processing cycles take priority within the Processor. The IsaGraf Sleep Period is the time frame between IsaGraf cycles. It is the period used for scanning the Trusted Communication Interface Modules, but it only applies when these are the only modules in the system and no other modules are present. The value entered here must be sufficient to allow all the Communication Interfaces used in the Trusted System to be scanned. As a rule of thumb, a minimum of 32 ms must be entered.

The default value for the Maximum Scan Time is 1000 ms. The value entered must be less than the Process Safety Time allocated to the Trusted System for the Plant, but greater than the scan time of the application program. If the value set is exceeded by the application program scan, the Trusted System will shutdown to its fail safe state. Note that Processor hot swaps and online updates can significantly extend the scan time, and it is recommended to set the maximum scan time to approximately four times the ‘current’ scan time as displayed in the Toolset Debugger Window.

3.1.6. Chassis Section

The figure entered against Max Racks is the number of chassis that will be used in the System and must include the Controller Chassis plus any local and / or remote Expander Chassis.

3.1.7. InterRange Instrumentation Group (IRIG)

Later versions of the TMR Processor are able to receive InterRange Instrumentation Group (IRIG) signals. For this to be active, the Processor Interface Adapter Unit (IRIG-B, model T8121 or T8123) must be fitted to the rear of the Controller Chassis. This contains the IRIG-B 'dongle'. The Check to Enable box in the InterRange Instrumentation Group (IRIG) area of the display must be selected. The user may also select which mode (IRIG-B002 or IRIG-B122) is required and also enable LED monitoring. If LED Monitoring is selected, the User 2 LED on the Front Panel of the Processor will flash to indicate that a valid IRIG signal is detected (once per second).

IRIG-B122 is the 1 - kHz amplitude modulated version of the signal.

IRIG-B002 is the RS485/422 version of the signal.

Note that configuring the above system configuration options and fitting/wiring the appropriate adapter unit is all that is required to ensure that the IRIG signals are assigned to the system clock. There is no need to add any programming to manipulate the Main Processor (MP) complex I/O definition boards TTMRP_3, TTMRP_4 and TTMRP_5 to synchronise the time. However, the IRIG signal does not contain any year information, and so an initial approximate setting of the real time clock will be necessary to enter the correct year.

The IRIG time source needs to be set up to output the same IRIG code as the TMR Processor is set up to receive. Some IRIG sources will output IRIG-B002 as TTL levels. This will not work with the TMR Processor, so ensure that the IRIG source is set to IRIG-B002 at 485/422 levels.

Some IRIG sources will have IRIG-B123 or B003 outputs. These have the time encoded in Straight Binary Seconds (SBS) at the end of the usual B122/002 message. These can be used with the TMR Processor because it ignores the SBS part of the message if there is one.

With the TMR Processor and the IRIG source set correctly, the time should be updated from the IRIG source once the module has booted. If the TMR Processor is not decoding the IRIG signal correctly for whatever reason, the System Health LED will flash red and the following will appear in the MP log:

```
48 IRIG: Maximum update interval exceeded
```

Typing `IRIG S` from the MP diagnostics will list the status of the IRIG Port.

Typing `IRIG I` from the MP diagnostics will give a detailed list of the IRIG Registers. The most useful is the Status Register, which can be decoded as follows:

Bit	Description
7	(Zero)
6	(Interrupt valid)
5	No License (goes low when valid IRIG dongle license found)
4	Control fields available, high when data found in control fields
3	Time valid (Only valid for that second)
2	IRIG-B122 input present (can sometimes be asserted erroneously)
1	IRIG-B002 input present
0	(Interrupt enable)

The IRIG-B signal is a pulse width modulated signal that transmits 100 pulses per second. For the IRIG-B002 signal this is directly output at RS422 levels. For the IRIG-B122 signal this pulse train is amplitude modulated onto a 1 kHz carrier.

The TMR Processor can accept IRIG-B122 inputs with a level between 0.25 V to 10 V PK-PK for the mark signal, although at 0.25 V it may be very close to the noise margin.

The TMR Processor accepts the IRIG-B002 signal at RS422 levels. RS422 is a differential signal pair. A signal level of about 1.5 V should be measurable across the termination resistor.

3.1.8. Additional User Serial Ports

Later versions of the TMR Processor are also fitted with three serial communications ports. These ports may only be accessed via a Processor Interface Adapter Unit (T812X), if this is fitted to the rear of the chassis. The values shown in the Additional User Serial Ports Window of the display are the default values. They may be edited to suit user requirements as necessary.

RS485fd = full duplex for point to point

RS485fdmux = full duplex for multidrop

RS485hdmux = half duplex (2 wire) for multidrop

The Protocols area can be used to configure the three ports to respond as slaves to Modbus protocol. On selecting Modbus, a Main Processor Modbus Slaves Window is displayed. Three slaves are available, one allocated to each port. Check Use This Slave to enable a slave, and save the Slave Address.

Once all required data has been entered, the user must select the OK button to enter the data in the System.INI file.

3.2. Complex I/O Equipment Definition

All Trusted Systems require a Processor definition in the I/O Connection Table. Details of how to edit the I/O Connection Table are given in PD-T8082. The structure of the definition is given below.

3.2.1. I/O Complex Equipment 'TTMRP'

DESCRIPTION

Trusted TMR Processor. This definition will open a single TMR Processor module. Only one installation is allowed. The data attached will give the application access to the user LEDs, real time clock and external analogue data from the system.

OEM PARAMETERS

OEM parameter	Valid numbers	Description
TICS_CHASSIS	1 – 15	The TICS chassis a slot number where the TMR Processor module is placed.
TICS_SLOT	0	

CONFIGURATION

Physical Module

RACK 1: [TTMRP_0]

16 ANALOGUE Inputs

Channel 1:	Module temperature (tenths of degrees C)
Channel 2	24 Vdc feed 1 after protection diodes (mV)
Channel 3	24 Vdc feed 2 after protection diodes (mV)
Channel 4	FRCA 8 Vdc supply (mV)
Channel 5	FRCB 8 Vdc supply (mV)
Channel 6	FRCC 8 Vdc supply (mV)
Channel 7	16-bit scan count
Channel 8	16-bit scan count
Channel 9	Number of locked variables in the application
Channels 10 – 16	Reserved

Note: The signals on channels 1 to 6 are generated from FCR D and can give incorrect values on the failure of FCR D. These values are for indication only and should not be used as part of the safety function.

RACK 2: [TTMRP_1]

16 BOOLEAN Inputs

Channel 1	PSU-A Output Status TRUE = Fail, FALSE = Pass
Channel 2	PSU-B Output Status TRUE = Fail, FALSE = Pass
Channel 3	PSU-A Line Status TRUE = Low Voltage Warning, FALSE = OK
Channel 4	PSU-B Line Status TRUE = Low Voltage Warning, FALSE = OK
Channel 5	IRIG Input Status TRUE = Pass, FALSE = Fail
Channel 6	System Health TRUE = Fail, FALSE = Healthy
Channel 7	Reset Pushbutton Status TRUE (one-shot) = pressed
Channel 8	Keyswitch Status TRUE = Run, FALSE = Maintain
Channel 9 - 16	Not used

RACK 3: [TTMRP_2]

16 BOOLEAN outputs

Channel 1	This channel drives the USER LED 1. TRUE = USER LED 1 ON, FALSE = USER LED 1 OFF
Channel 2	This channel drives the USER LED 2. TRUE = USER LED 2 ON, FALSE = USER LED 2 OFF
Channel 3	Unlock all channels, edge triggered on a (FALSE -> TRUE) change
Channel 4	System Healthy LED controls. TRUE = Unhealthy, FALSE = Healthy.
Channel 5	USER LED 1 Colour. TRUE = Green, FALSE = Red.
Channel 6	USER LED 2 Colour. TRUE = Green, FALSE = Red.
Channels 7 – 16	Not used

RACK 1:	1 ANALOGUE Input	TMR Interface status. See "TMR Interface Status word format" in EXTRA INFORMATION for description of data
RACK 2:	16 ANALOGUE Inputs	Each variable contains data on the transceivers connected to the TMR Interface. Variable 1 is Regent chassis 1, Variable 16 is Regent chassis 16. See "Transceiver variable" in EXTRA INFORMATION for detailed data structure.

RACK 4: [TTMRP_3 – Real time clock input rack]

6 ANALOGUE inputs

Channel 1	Year
Channel 2	Month
Channel 3	Day of month
Channel 4	Hours
Channel 5	Minutes
Channel 6	Seconds

If the RTC read channel, Channel 2, of TTMRP_5 is set to TRUE, this input rack is refreshed every cycle to hold the current date and time.

RACK 5: [TTMRP_4 – Real time clock program rack]

6 ANALOGUE outputs

Channel 1	Year
Channel 2	Month
Channel 3	Day of month
Channel 4	Hours
Channel 5	Minutes
Channel 6	Seconds

This output rack (above) allows the application writer to specify a new time and date to be written to the RTC by the RTC control rack described below. It does not perform the write itself.

RACK 6 [TTMRP_5 – Real time clock control rack]

7 BOOLEAN outputs

Channel 1	RTC Write
	TRUE = Set RTC if previously FALSE
	FALSE = no associated action

Channel 2	RTC Read TRUE = Refresh RTC on every subsequent cycle False = Stop RTC input rack refreshes for every subsequent cycle.
Channel 3	Set year
Channel 4	Set month
Channel 5	Set day of month
Channel 6	Set hours
Channel 7	Set minutes
Channel 8	Set seconds

This output rack physically writes the date and time components assigned to the RTC program rack to the RTC. The write operation is performed in the event of a rising edge on the RTC write channel, Channel 1. The set channels, Channels 3 – 8, determine which date and time values to write, i.e. only date/time components that have a corresponding TRUE set channel are written to the RTC. Other date/time components remain unchanged. The date/time is only written to the RTC if the resulting date/time is valid, otherwise a run-time error is generated. The RTC read channel, Channel 2, enables/disables refreshes of the RTC input rack on every subsequent cycle.

RACK 7: (INFO)

11 INTEGER inputs

Channel 1	Chassis position of AM
Channel 2	Slot position of AM 0 – Left 1 – Right
Channel 3	Indication of global health of AM 1 – No slice errors 0 – An error has been found
Channel 4	Current state of AM
Channel 5	Chassis position of SM

Channel 6	Slot position of SM 0 – Left 1 – Right
Channel 7	Indication of global health of SM 1 – No slice errors 0 – An error has been found
Channel 8	Current state of SM
Channel 9	Slice information of SM – see **Note**
Channel 10	Reserved
Channel 11	Reserved

APPENDIX:

Note:	Bit 0	AM slice A: 1 - Slice is responding and there are no slice errors. 0 - Slice is either NOT responding or there is a slice error.
	Bit 1	AM slice B: 1 - Slice is responding and there are no slice errors. 0 - Slice is either NOT responding or there is a slice error.
	Bit 2	AM slice C: 1 - Slice is responding and there are no slice errors. 0 - Slice is either NOT responding or there is a slice error.
	Bit 3	AM ejectors open: 1 - AM ejectors open. 0 - AM ejectors closed.
	Bit 4	SM slice A: 1 - Slice is responding and there are no slice errors. 0 - Slice is either NOT responding or there is a slice error.
	Bit 5	SM slice B: 1 - Slice is responding and there are no slice errors. 0 - Slice is either NOT responding or there is a slice error.
	Bit 6	SM slice C: 1 - Slice is responding and there are no slice errors. 0 - Slice is either NOT responding or there is a slice error.
	Bit 7	SM ejectors open: 1 - SM ejectors open. 0 - SM ejectors closed.

3.3. Inter-Module Bus

Each Processor FCR contains a Bus Interface to the Inter-Module Bus. The triplicated Inter-Module Bus provides communication interconnection between modules in the Trusted Controller Chassis, at a data transfer rate of up to 150 Mbaud.

The Inter-Module Bus handles the following triplicated signals:

Data	8-bit, bi-directional bus.
Control	Bus clocks, module enables and bus direction control.
System Watchdog	A dynamic signal indicating the correct processing of safety critical data. The signal is generated by the hardware watchdog signal from each Processor.
Power Fail	Indicating a power fault in the associated FCR.
Active/Standby	Status line between the active/standby Trusted TMR Processors that are used for negotiating the active/standby state.
Slot	Indicating the left or right Trusted TMR Processor slot position to the Processor.
System ID	A 4 bit code indicating the system address to the Processor.

Additionally, a Chassis Connection signal is provided for grounding the module electromagnetic interference shield.

3.3.1. Processor Memory Voting Bus

The Processor memory voting bus is 32-bits wide and provides real time voting of memory read cycles.

3.3.2. Inter-Module Bus Voting Bus

Data received from the Inter-Module Bus is processed via an independent voting bus. This bus protects the three Processor FCRs from a data fault, by exchanging data between them and the Front Panel FCR.

3.3.3. Processor Voting Bus

The Processor voting bus is a serial bus that provides fault protection for certain types of FCR signals.

3.3.4. Front Panel Voting Bus

The Front Panel voting bus provides the following functions:

- Voted watchdog signal to the Front Panel for indicating Processor faults.

- Voted serial data to the Front Panel for communications, Front Panel indicators, etc.
- Protected serial data from the Front Panel for communications, Front Panel status, etc.

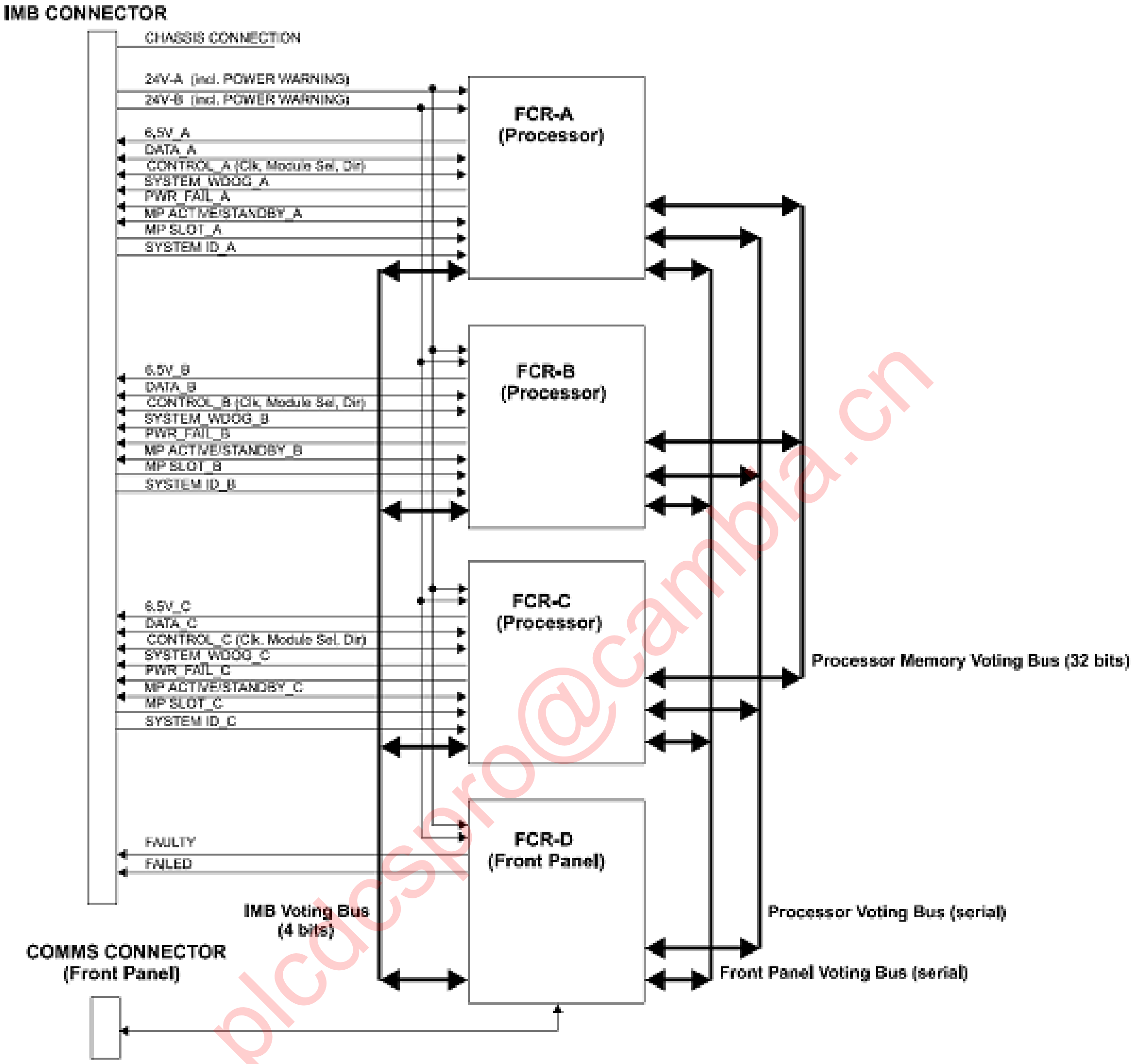

Figure 3 Functional Block Diagram showing Trusted TMR Processor Communications

3.4. Isolation

All signals exchanged between FCRs are protected to prevent the propagation of faults between independently powered FCRs.

The Front Panel diagnostics port is electrically isolated from the Front Panel FCR.

The Processor and Front Panel FCR provide electrical isolation for the 24 Vdc power feed in addition to the POWER WARNING signal.

4. Operation

On power-up, the Trusted TMR Processor initialises its local resources and determines their operability. This includes verification of memory, arithmetic and logic units, timers and all fault detection mechanisms.

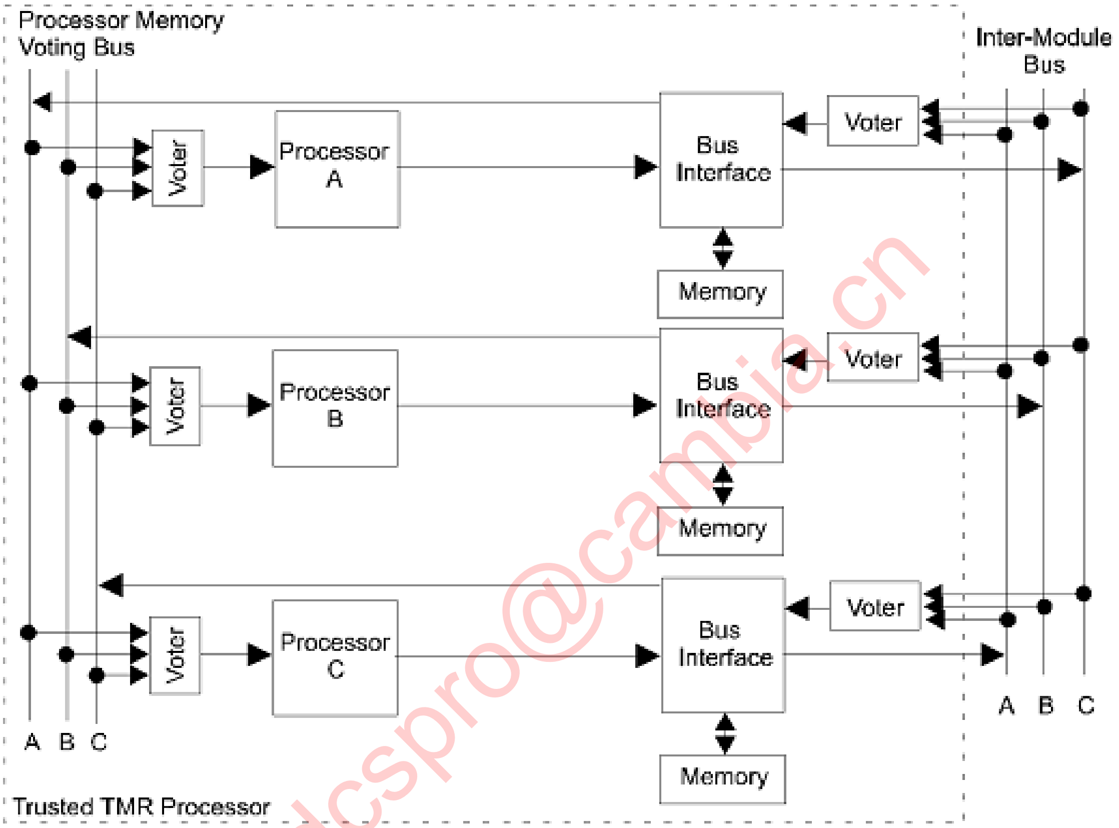

Figure 4 Block Diagram of Module Operation

The voter circuits read the input data from the Inter-Module Bus and carry out a continuous 2oo3 vote of the data.

The voting and fault detection circuits enable the module to identify and isolate transient, intermittent and permanent faults as they occur. All faults are recorded in the system's fault history. Permanent faults are also annunciated by an LED on the module Front Panel and by the Fault/Fail relay circuits to external indicator systems.

The input data is processed by the Bus Interface, checked for errors and I/O module faults before being transmitted to the Processor memory voting bus. The data is 2oo3 voted by voter circuits before passing to the Processors.

Each Processor executes synchronously the application program with the other two Processors. At the same time, all process state input data, internal data and application program instructions are also voted. Output data from the Processors is transmitted via the Bus Interface to the Inter-Module Bus.

The output data from each of the module's three Processors is then transmitted to the output module.

In the output module, voter circuits perform discrepancy checks on the data. As long as there are no discrepancies between the data, operation continues normally. If a voter circuit detects that the data it receives from one Processor is not the same as that being transmitted from the others, the Trusted TMR Processor reverts to 2oo3 operation and its error indicator is set.

4.1. System Overheads

In addition to running application programs, the Trusted TMR Processor takes care of system overheads, (such as background diagnostics), including voter tests, read tests of the Erasable Programmable Read Only Memories (EPROMs) and read-write tests of the Random Access Memory (RAM).

4.2. Online Operator Inputs

Online adjustment of system operating parameters, e.g. set points, loop tuning and time delays, and operator commands, e.g. reset and override, within defined safe operational limits, is available during the 'Maintenance' mode of the Trusted TMR Processor using the Engineering Workstation.

4.3. Standby Processor

A second Trusted TMR Processor can be installed in a system to act as the standby Processor in a Companion Slot configuration. This option allows an additional Trusted TMR Processor to be available for use should the active module need to be functionally replaced. The standby module runs its normal internal diagnostic tests in standby mode, and is constantly updated by the active Trusted TMR Processor. Transition from standby to active mode is triggered by the active module. See section 5.3 for further information.

4.4. Module Management

The system firmware is loaded via the bootstrap monitor. The Trusted TMR Processor configuration information is held in the non-volatile memory.

The Trusted TMR Processor can be configured by one of two methods:

- Engineering Workstation via the Front Panel diagnostics port.
- Engineering Workstation via the Trusted Communication Interface.

Where both active and standby Trusted TMR Processors are installed, a bumpless changeover between the modules is performed automatically. Any changeover is logged in the system event log.

When a new module is inserted, it is automatically synchronised and educated by the two 'good' channels of the faulted module being replaced.

Two interlock switches are provided on the top and bottom module latches to detect removal of the module. Switch actuation generates an interrupt for each Processor.

Note: Releasing the active Trusted TMR Processor's ejector levers in an active/standby configuration, will cause an automatic changeover between the active and standby Trusted TMR Processors to occur.

4.5. Security

IEC 61131 TOOLSET password protection, with corresponding levels of access permission, and the Front Panel Keyswitch are used to prevent unauthorised access to the system.

4.6. Front Panel

Figure 5 shows the physical features of the Trusted TMR Processor. The Front Panel of the Trusted TMR Processor has status and diagnostic indicator LEDs, a reset button and a Maintenance Enable Keyswitch.

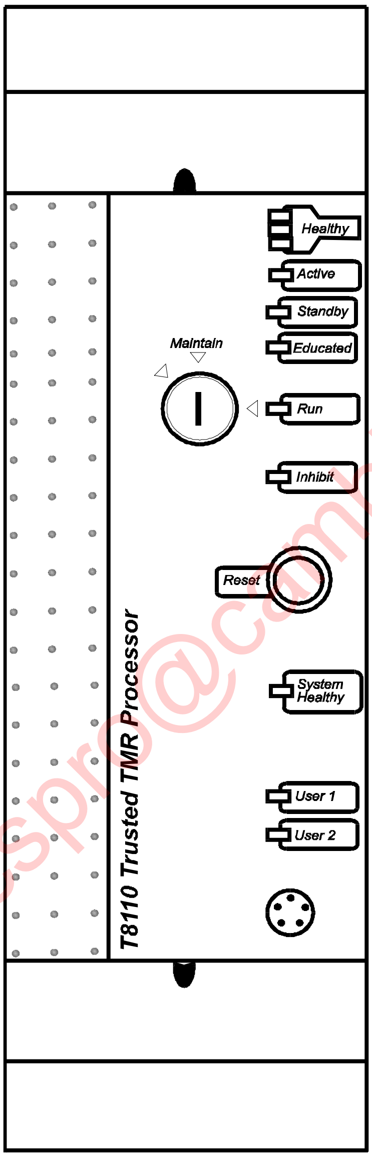

Figure 5 Module Front Panel

4.7. Module Status LEDs

There are eleven status LEDs on the Processor Front Panel; three Healthy, one Active, one Standby, one Educated, one Run, one Inhibit, one System Healthy, and two User. The Healthy indicators are controlled directly by each module slice. All LEDs are controlled by the FPU. The FPU receives data from each of the module slices. The Front Panel Unit (FPU) performs a 2oo3 vote on each data bit from the slices and sets the indicators accordingly.

The module status LED states and their meanings are described as follows:

LED	INDICATION
Healthy	Overall health of each Processor slice: Steady green: healthy Steady red: slice failed.
Active	Steady green when the Processor is in the Active mode.
Standby	Steady green when the Processor is in the Standby mode. Flashing green when the Processor has changed from the Active to the Standby mode.
Educated	Steady green when the Processor is Educated. Flashing green when the Processor is being Educated. Off when the Processor is not Educated, or the application program has stopped.
Run	Flashing green when the Processor is operating normally with full integrity. Steady green in Standby. Off when the application program in the Active Processor has stopped.
Inhibit	Flashing green when any input or output is locked. This LED also flashes green if a changeover from Active to Standby is attempted when the current Standby Processor is fitted with a different system configuration.
System Healthy	System health: Steady green healthy Flashing red system boot-up, system fault, self-test fail, Inter Module Bus (IMB) error. Trusted I/O module error, Active/Standby module failing to respond, module slice error, channel fault, or a module is being simulated. Regent I/O module error, module failing to respond. Off: illegal state
User 1 and User 2	General purpose red LEDs for use under software control.

Note: If the Healthy LED is flashing green and power is switched off, then on again, the associated slice may fail to operate. When the Healthy LED is flashing red, processing is automatically switched to the Standby Processor. The faulty Processor must be replaced.

4.7.1. Reset Button

The fault Reset button clears all recorded faults, resets all fault counters and requests all modules to do the same. Fault testing continues, and faults that are still present will be recorded again. The fault reset can also be initiated from the Engineering Workstation by personnel who are authorised by the appropriate passwords, to implement maintenance changes to a Trusted System.

Note that although pressing the Reset button will make the system look healthy, it may erase faults that take many hours to be recorded again. It is recommended to note the fault code (which appears at the bottom of the HKEEPING board in each module's complex equipment definition, see the module PD and PD-8032B) before pressing Reset.

4.7.2. Maintenance Enable Keyswitch

The two position keyswitch is used to select the following modes:

- Run
- Maintenance

In the 'Run' position: the memory is locked.

In the 'Maintain' position: the keyswitch allows the download of application programs by the Engineering Workstation, together with the appropriate access permission.

Note To prevent unauthorised use, the key can be removed with the keyswitch in either position.

4.8. Composite Scan Time Estimation (pre TÜV release 3.5)

The Composite Scan time for a Trusted System represents the time required to read the input data, solve the application logic, and write the output data. This sequence is repeated cyclically for as long as the Trusted system is executing an application. For convenience, the above cyclical sequence is broken down into four discrete elements: Central Modules, Input Modules, Output Modules, and the Application. The estimated Composite Scan time is the sum of these four elements.

The calculations here apply to systems before TÜV release 3.5. At release 3.5 the execution times have been significantly improved. For systems from release 3.5, refer to section 4.9.

4.8.1. Central Modules

The Central Module time is based on the number and type of central Trusted Modules. It is calculated by multiplying the number of installed modules by the appropriate time factor, then adding the results.

Module Type	No. Installed	Time	
Standby TMR Processor Module		x 4 ms	
TMR Interface Module		x 15 ms	
Communications Interface Module		x 4 ms	
		Central Module Total	

The Central Modules also contribute to the Input Module and Output Module times. The impact to each is factored in on a per-module basis, and is included in the respective calculations as the "Scan Factor".

Module Type	No. Installed	Time	
Standby TMR Processor Module		x 1 ms	
TMR Interface Module		x 0.81	
Communications Interface Module		x 1.5 ms [1]	
		Scan Factor	

4.8.2. Input Modules

The Input Module time is based on the number of Trusted High Density Input Modules. The time calculations are independent of the number of channels on each Module (i.e. a 60 channel DUAL Module has an equivalent input Module time as a 40 channel TMR Module). The Input Module time is calculated by adding the "Scan Factor" to a constant, then multiplying this by the total number of High Density Input Modules.

Scan Factor	No. Input Modules	Input Total
(+ 4.5 ms) x		

[1] The actual values used in calculating the "Scan Factor" for the TMR Interface and Communication Interface Modules can vary. The values presented in the above table are correct for the default configuration, but can be adjusted downward to tune system performance.

4.8.3. Output Modules

The Output Module time is based on the number of Trusted High Density Output Modules. The time calculations are independent of the number of channels on each Module (i.e. a 32 channel 120 Vdc Digital Output Module has the same output Module scan time as a 40 channel Analogue Output Module). The Output Module time is calculated by multiplying the “Scan Factor” by 2, adding the result to a constant, then multiplying by the total number of High Density Output Modules.

Scan Factor	No. Input Modules	Input Total
((x 2) + 7.6 ms) x		

While the Output Module time may seem disproportionately long when compared to the Input Module time based solely on the number of modules, Output Modules are accessed twice during each cyclical period: once to provide input data to the application (such as channel state, voltage, and current), and again when controlling the outputs themselves.[2]

4.8.4. Application Execution

The Application Execution time is based on the estimated size of the application. While actual application size varies greatly based on numerous factors, an estimation of the application size can generally be calculated based on the number of I/O points in a system. The Application Execution time is calculated by adding a constant overhead factor to the total number of I/O modules, then multiplying by a constant time factor.

No. I/O Modules	Application Execution Total
(+ 5) x 1.5 ms	

If the size of the application is known, or if it can be derived from the application size of a similar system, the Application Execution time can be calculated directly by multiplying the application size by a constant time factor.

Size of the Application (in KB)		Application Execution Total
	x 0.3 ms	

[2] The default configuration is for all outputs to be updated each scan, irrespective of a change of state (or value). If the Trusted System is configured to update outputs only when they change, the Output Module time calculation is as follows: [(Scan Factor + 4.5 ms) x No. Output Modules] + [(Scan Factor + 3.1) x DeltaOM], where “DeltaOM” represents the average number of Output Modules with at least one channel that will change state (or value) with each composite scan time and is at least 1 for any system that contains at least 1 Output Module.

4.8.5. Composite Scan Time

The Composite Scan time is the sum of the Central Module time, Input Module time, Output Module time, and the Application Execution time.

Central Module Total	
Input Module Total	
Output Module Total	
Application Execution Total	
Composite Scan Time	

The default configuration is for all outputs to be updated each scan, irrespective of a change of state (or value). If the Trusted System is configured to update outputs only when they change, the Output Module time calculation is as follows: [(Scan Factor + 4.5 ms) x No. Output Modules] + [(Scan Factor + 3.1) x DeltaOM], where “DeltaOM” represents the average number of Output Modules with at least one channel that will change state (or value) with each composite scan time and is at least 1 for any system that contains at least 1 Output Module.

4.8.6. Example Calculation

As an example, consider a simple Trusted System with the following configuration:

Part No.	Description	Qty.	Type
T8110B	Trusted TMR Processor	1	N/A
T8151B	Trusted Communication	2	Central
T8403	Trusted TMR 24 Vdc Digital Input	4	Input
T8431	Trusted TMR Analogue Input	1	Input
T8451	Trusted TMR 24 Vdc Digital Output	2	Output

This is a relatively small system with 280 I/O points and 2 communication modules.

Module Type	**No. Installed**	**Time**	
Standby TMR Processor Module	0	x 4 ms	0 ms
TMR Interface Module	0	x 15 ms	0 ms
Communications Interface Module	2	x 4 ms	8 ms
		Central Module Total	**8 ms**

Module Type	**No. Installed**	**Time**	
Standby TMR Processor Module	0	x 1 ms	0 ms
TMR Interface Module	0	x 0.8 ms	0 ms
Communications Interface Module	2	x 1.5 ms	3 ms
		Scan Factor	**3 ms**

Scan Factor	**No. Input Modules**	**Input Total**
(3 ms + 4.5 ms) x	5	**37.5 ms**

Scan Factor	**No. Output Modules**	**Output Total**
((3 ms x 2) + 7.6 ms) x	2	**27.2 ms**

No. I/O Modules	**Application Execution Total**
((7 + 5) x 1.5 ms)	**18 ms**

Central Module Total	**8.0 ms**
Input Module Total	**37.5 ms**
Output Module Total	**27.2 ms**
Application Execution Total	**18.0 ms**
Composite Scan Time	**90.7 ms**

4.9. Composite Scan Time Estimation (from TÜV release 3.5)

The Composite Scan time for a Trusted System represents the time required to read the input data, solve the application logic, and write the output data. This sequence is repeated cyclically for as long as the Trusted System is executing an application. For convenience, the above cyclical sequence is broken down into four discrete elements: Input Modules, Output Modules, Application and Communications. The estimated composite scan time is the sum of these four elements.

The calculations here apply to systems from TÜV release 3.5. For systems before release 3.5, refer to section 4.8.

4.9.1. Input Modules

The Input Module time is based on the number of Trusted High Density Input Modules. The time calculations are independent of the number of channels on each Module (i.e. a 60 channel DUAL Module has the same Input Module time as a 40 channel TMR Module). The Input Module time is calculated by multiplying a time factor by the total number of High Density Input Modules. Digital and analogue Modules have the same time factor.

The Input Module time may be reduced by setting individual modules to scheduled polling in their entry in the System.INI configuration. As an approximation, this will reduce their scan time effect in proportion to their poll interval.

Scan Factor	No. Input Modules	Input Total
4.5 ms x		

4.9.2. Output Modules

The Output Module time is based on the number of Trusted High Density Output Modules. The time calculations are independent of the number of channels on each Module (i.e. a 32 channel 120 Vdc Digital Output Module has the same output Module scan time as a 40 channel Analogue Output Module). The Output Module time is calculated by multiplying a time factor by the total number of High Density Output Modules.

The Output Module time may be reduced by setting individual modules to scheduled polling in their entry in the System.INI configuration. This spaces out the read operations from the module. As an approximation, this will reduce two-thirds of their scan time effect in proportion to their poll interval. The remaining time is due to write operations to the module. Selecting ‘write by exception’ in the entry in the System.INI configuration will prevent write operations if the outputs have not changed.

Scan Factor	No. Output Modules	Output Total
7 ms x		

4.9.3. Application Execution

The Application Execution time has a minimal effect on the total scan time. It is based on the processing load of the application. While actual application load varies greatly based on numerous factors, an estimation can generally be calculated based on the number of I/O modules in a system. The Application Execution time is calculated by multiplying the total number of I/O modules by a constant time factor.

No. I/O Modules	Application Execution Total
( ) x 0.3 ms	

If the size of the application is known, or if it can be derived from the application size of a similar system, the Application Execution time can be calculated directly by multiplying the application size by a constant time factor.

Size of the Application (in KB)		Application Execution Total
	x 0.05 ms	

4.9.4. Communications

Communications is less easy to calculate, because it can be sporadic and depends heavily on the details of the configuration. The estimate used in section 4.8 may be used as a rough guide, based on the I/O module count in the way it affects data volume.

No. I/O Modules	No. Comms Modules	Communications Total
( ) x 1.5 ms x	( )	

A small improvement in I/O scanning time may be possible if unused slots are disabled in the system configuration. This will have most effect on systems with many chassis but few modules, e.g. where each chassis is sited at an outstation with one input and one output module. If a slot is disabled on a release 3.5 System, the Processor ignores it altogether. Note that one unused slot should be left in service for diagnostic interrogation of suspect modules.

4.9.5. Example Calculation

As an example, consider a simple Trusted System with the following configuration:

Part No.	Description	Qty.	Type
T8110B	Trusted TMR Processor	1	N/A
T8151B	Trusted Communication	2	N/A
T8403	Trusted TMR 24 Vdc Digital Input	4	Input
T8431	Trusted TMR Analogue Input	1	Input
T8451	Trusted TMR 24 Vdc Digital Output	2	Output

This is a relatively small system with 280 I/O points and 2 communication Modules.

Scan Factor	No. Input Modules	Input Total
4.5 ms x	5	**22.5**

Scan Factor	No. Output Modules	Output Total
7 ms x	2	**14**

No. I/O Modules	Application Execution Total
(7) x 0.3 ms	**2.1**

No. I/O Modules		No. Comms Modules	Communications Total
(7)	x 1.5 ms x	(2)	**21**

Central Module Total	**22.5 ms**
Input Module Total	**14 ms**
Output Module Total	**2.1 ms**
Application Execution Total	**21 ms**
Composite Scan Time	**59.7 ms**

This assumes all modules are polled every scan, all outputs are written every scan and communications is moderate to heavy. The time may be shortened using scheduled polling, write by exception and rationalised communications. Note that the Application Execution time is insignificant.

5. Fault Finding and Maintenance

5.1. Testing and Diagnostics

The Trusted TMR Processor provides fault monitoring, self-test and diagnostics functions for the Trusted TMR processing sub-system.

Periodic hardware tests are carried out on the microprocessors, memory management units, clock devices and communications busses.

The Trusted TMR Processor’s error detection logic is tested periodically to ensure its continued correct operation. Testing is performed using hardware and software self-tests that are automatically scheduled by the module’s real-time operating system.

The results of all testing are stored in a log for uploading to an Engineering Workstation.

The module’s ‘Maintenance’ mode provides all of the functionality available during the ‘Run’ mode, with provision to download application programs.

In the Maintenance mode, the Engineering Workstation is allowed to modify user programs and re-program the module.

The Trusted TMR Processor has an RS232 serial diagnostics port and Front Panel indicators to aid module fault diagnosis.

The diagnostics port has a serial data rate of 19k2 bits/s and is used to interface the Engineering Workstation to the Trusted TMR Processor.

5.2. Faults

In the event of a second processor board failure occurring, the Trusted TMR Processor is isolated automatically from the remaining system operation. External interfaces are held in their default condition, except where the interface is used for fault and diagnostic information. Where possible, information indicating the source/cause of failure is retained in the non-volatile memory. A fault reset command can be initiated either by the Front Panel Reset push-button or from the Engineering Workstation.

In an active/standby configuration (Companion Slot), on the first processor slice board failure an active/standby Trusted TMR Processor changeover will occur automatically providing the prerequisites have been met as described in the next section.

The power fail signals provide early notification of an impending supply failure, if this arises the Trusted TMR Processor goes into the ‘Power Off’ mode.

System data, fault information and user program data are retained in the Trusted TMR Processor non-volatile memory during ‘Power Off’ mode. User program data (such as internal and plant status information) is available to the user programs in ‘Online’ and ‘Test and Load’ modes.

5.3. Transfer between Active and Standby Processor Modules

CAUTION:

Under no circumstances remove a Module that is indicating Active Mode. Removal of an Active Module may result in Modules within the Chassis adopting their default (shutdown) state, and initiate shutdown states via the application program.

Note: In the following procedure it is assumed that the current Active Module has developed a fault and the replacement Module does not have same System.INI configuration file as the Active Module.

The user will define the primary processor location as part of the complex equipment definition within the IEC 61131 TOOLSET. This will always be defined as chassis 1 slot 0, secondary processor locations are never defined in either the Configuration Manager or the IEC 61131 TOOLSET.

Active / Standby changeovers will be inhibited if any I/O has been forced on the System. This will be indicated by the Inhibit LED on the Active Processor flashing green, prior to insertion of the Standby Processor.

- The replacement Processor Module must be inserted in the vacant Processor slot, ensuring that the Module is correctly located and the ejector tabs are closed. The newly installed Module will perform its power-up sequence.

  Ensure that the LED indicators on the newly installed module are as follows:

LED 1	Healthy A	Steady Green
LED 2	Healthy B	Steady Green
LED 3	Healthy C	Steady Green

  Once initialised, the newly installed Processor Module will be set to Standby Mode. A connection will be established between the new Standby Module and the Active Module. The Active Module will prepare and write data to educate the Standby Module. Standby Module education is indicated by the Education LED on the Standby Module being steady green. Hand-over at this point is inhibited, indicated by the Inhibit LED on the Active Module flashing green.

- At this point the Standby Module needs to be removed and re-inserted.

  Open the Standby Module ejector tabs and remove the Standby Module.

- Plug in the Standby Module again, ensuring that the Module is correctly located and the ejector tabs are closed.

  On second insertion the Standby Module will initialise and be set to Standby Mode. A connection to the Active Module will again be made and again data will be prepared and written to educate the Standby Module. However, this time the new Module will be configured as the Active Module, and therefore hand-over will be allowed. The Inhibit LED on the Active Module will change to steady green.

Changeover will now take place automatically, with the new Module taking over as the Active Module and the faulty Active Module becoming the Standby. The Active LED on the new Active Module will be steady green.

The Active LED on the original Active Module will go out and the Standby LED will be steady green. The faulty channel will be indicated by the respective Healthy LED flashing red.

- The Standby Module (the original faulty Active Module) can now be removed.

Note: A non-faulty Active Module can be replaced by plugging in a replacement Module. Once the replacement Module has been initialised as the Standby, changeover can be initiated by opening the ejector tabs on the Active Module or using commands via the diagnostic interface. Changeover will take place automatically, with the new Module taking over as the Active.

Page intentionally left blank

6. Specifications

Voltage Range	20 Vdc to 32 Vdc
Maximum Load	80 W
Heat Dissipation	80 W
Use with Chassis	T8100
Processor Clock	100 MHz
Memory Type and Size	
DRAM	16 MB EDO 60 ns
EPROM	512 kB
FLASH	2 MB
NVRAM	128 kB
Retained Variable Storage	4 KB
Each variable requires:	
Booleans	1 byte
Analogues	4 bytes
Timers	5 bytes
SOE Buffer Size	1000 events, transferred to CI buffer of 4000 events
I/O Interface	Triple redundant Inter-Module Bus
Operating Temperature	0 °C to 60 °C (32 °F to 140 °F)
Non-operating Temperature	-25 °C to 70 °C (-13 °F to 158 °F)
Relative Humidity range (operating, storage & transport)	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	2.94 kg (6.48 lb)