ics triplex

8000 SERIES TMR SYSTEM

OPERATOR AND MAINTENANCE MANUAL

DOCUMENT NUMBER 552864

ISSUE 02 JUNE 2004

Printed in England

This page intentionally blank

Issue Record

Issue		Revised by	Checked by	Authorised by
Number	Date			
Issue 1	May	J Bourn		
Issue 2	June	N Owens		

NOTICE

The information contained in this document is subject to change without notice. The reader should, in all cases, consult ICS Triplex Technology Ltd. to determine whether any such changes have been made. From time to time, amendments to this document will be made as necessary and will be distributed by ICS Triplex Technology Ltd.

Information in this documentation set may be subject to change without notice and does not represent a commitment on the part of ICS Triplex Technology Ltd.

The contents of this document, which may also include the loan of software tools, are subject to the confidentiality and other clause(s) within the Integrator Agreement and Software License Agreement.

DISCLAIMER

The illustrations, figures, charts, and layout examples in this manual are intended solely to illustrate the text of this manual.

The user of, and those responsible for applying this equipment, must satisfy themselves as to the acceptability of each application and use of this equipment.

This document is based on information available at the time of its publication. While efforts have been made to be accurate, the information contained herein does not purport to cover all details or variations in hardware or software, nor to provide for every possible contingency concerning installation, operation, or maintenance. Features may be described herein which are not present in all hardware or software systems. ICS Triplex Technology Ltd. assumes no obligation of notice to holders of this document with respect to changes subsequently made.

ICS Triplex Technology Ltd. makes no representation or warranty, expressed, implied, or statutory with respect to, and assumes no responsibility for the accuracy, completeness, sufficiency, or usefulness of the information contained herein. No warranties of merchantability or fitness for purpose shall apply.

REVISION AND UPDATING POLICY

All new and revised information pertinent to this document shall be issued by ICS Triplex Technology Ltd. and shall be incorporated into this document in accordance with the enclosed instructions. The change is to be recorded on the Amendment Record of this document.

PRECAUTIONARY INFORMATION

WARNING

Warning notices call attention to the use of materials, processes, methods, procedures or limits which must be followed precisely to avoid personal injury or death.

CAUTION

Caution notices call attention to methods and procedures which must be followed to avoid damage to the equipment.

Notes:

Notes highlight procedures and contain information to assist the user in the understanding of the information contained in this document

WARNING

RADIO FREQUENCY INTERFERENCE

MOST ELECTRONIC EQUIPMENT IS INFLUENCED BY RADIO FREQUENCY INTERFERENCE (RFI). CAUTION SHOULD BE EXERCISED WITH REGARD TO THE USE OF PORTABLE COMMUNICATIONS EQUIPMENT AROUND SUCH EQUIPMENT. SIGNS SHOULD BE POSTED NEAR THE EQUIPMENT CAUTIONING AGAINST THE USE OF PORTABLE COMMUNICATIONS EQUIPMENT.

MAINTENANCE

MAINTENANCE MUST BE PERFORMED ONLY BY QUALIFIED PERSONNEL. OTHERWISE PERSONAL INJURY OR DEATH, OR DAMAGE TO THE SYSTEM, MAY BE CAUSED.

CAUTION

STATIC SENSITIVE DEVICES

MODULES IN THE TMR SYSTEM MAY CONTAIN STATIC SENSITIVE DEVICES WHICH CAN BE DAMAGED BY INCORRECT HANDLING OF THE MODULE. THE PROCEDURE FOR MODULE REMOVAL IS DETAILED IN RELEVANT PRODUCT DESCRIPTIONS AND MUST BE FOLLOWED. ALL TMR SYSTEMS MUST HAVE LABELS FITTED TO THE EXTERIOR SURFACE OF ALL CABINET DOORS CAUTIONING PERSONNEL TO OBSERVE ANTI-STATIC PRECAUTIONS WHEN TOUCHING MODULES.

RECORD OF AMENDMENTS

Issue Number	Changes
Issue 1	**Initial Issue**

TABLE OF CONTENTS

OPERATOR AND MAINTENANCE MANUAL

1. INTRODUCTION

1.1 MAINTAINING SAFETY

This manual should be read in conjunction with the safety manual (product number 8094)

1.2 OPERATION AND MAINTENANCE PLAN

This Operation and Maintenance requirement ensures that functional safety continues beyond the design, production, installation and commissioning of the system. The in-service operation and maintenance is normally beyond the system integrator responsibility. However, guidance and procedures shall be provided to ensure that the persons or organisations responsible for Operation and Maintenance maintain the intended safety levels.

The Operating and Maintenance Plan shall include the following:

- Although the TMR product requires no specific power-up and power-down requirements, it is possible that the project specific implementation will dictate specific action sequences. These sequences shall be clearly defined, ensuring that the sequences cannot result in periods of the system's inability to respond safely whilst a hazard may be present.
- The Maintenance Plan shall detail the procedures to be adopted when re-calibrating sensors, actuators and I/O modules. The recommended calibration periods shall also be included.
- The Maintenance Plan shall include the procedure to be adopted for testing the system, and the maximum intervals between manual testing.
- Sensor and actuator maintenance will require the application of overrides in certain circumstances. Where these are required, they shall be implemented in accordance with the guidance provided within this document.

1.3 PLANNED MAINTENANCE

In most system configurations there will be some elements that are not tested by the system's internal test facilities. These may be the final passive elements in some I/O modules types, the sensors and actuators themselves and the field wiring. A regime of Planned Maintenance testing shall be adopted to ensure that faults do not accumulate within those elements that could ultimately lead to the system's inability to perform its required safety functions. The maximum interval between these tests shall be defined during the system design, i.e. before installation. It is highly recommended that the test interval be less than 12 months.

1.4 FIELD DEVICE MAINTENANCE

During the lifetime of the system, it will be necessary to undertake a number of field maintenance activities that will include re-calibration, testing and replacement of devices. Facilities should be included within the system design to allow these maintenance activities to be undertaken. Similarly, the operating and maintenance plan needs to include these maintenance activities, and their effect on the system operation and design. In general, adequate provision for these measures will be defined by the client. Provided the facilities, i.e. maintenance overrides, are implemented within the requirements specified within this document, no further safety requirements are necessary.

It is highly recommended that the I/O forcing capability should NOT be used to support field device maintenance. This facility is provided to support application testing only. Should this facility be used, the requirements defined in para. 1.9 shall be applied.

1.5 MODULE FAULT HANDLING

When properly configured and installed, the TMR system is designed to operate continuously and correctly even if one of its modules has a fault. When a module does have a fault it should be replaced promptly to ensure that faults do not accumulate, thereby causing multiple failure conditions that could cause a plant shutdown. All modules permit live removal and replacement, and modules within a fault-tolerant configuration can be removed with no further action. Modules in a non-redundant or fail-safe configuration will require the application of override or bypass signals for the period of the module removal to ensure that unwanted safety responses are not generated inadvertently.

On-site repair of modules is not supported; all failed modules should be returned for repair and/or fault diagnosis. The return procedure for modules should include procedures to identify the nature and circumstances of the failure and the system response. Records of module failures and repair actions shall be maintained.

1.6 MONITORING

In order to establish that the safety objectives have been met through the lifetime of the system it is important to maintain records of the faults, failures and anomalies. This requires the maintenance of records by both the end-user and the system integrator. The records maintained by the end-user are outside the scope of this document; however, it is highly recommended that the following information be included:

- Description of the fault, failure or anomaly
- Details of the equipment involved, including module types and serial numbers where appropriate
- When the fault was experienced and any circumstances leading to its occurrence
- Any temporary measures implemented to correct or work around the problem
- Description of the resolution of the problem and reference to remedial action plans and impact analysis

Each system integrator should define the field returns, repair and defect handling procedure. The information requirements placed on the end user because of this procedure should be clearly documented and provided to the end user. The defect handling procedure shall include:

- Method of detecting product related defects and the reporting of these to the original designers.
- Methods for detecting systematic failure that may affect other elements of the system or other systems, and links to the satisfactory resolution of the issues.
- Procedures for tracking all reported anomalies, their work around and/or resultant corrective action where applicable.

1.7 DIAGNOSTIC ACCESS

The TMR Processor supports comprehensive diagnostic facilities. Some of these facilities have the capability of modifying the system’s operation and are therefore password protected, to provide access protection in addition to that afforded by physical access to the system.

The password is defined in the security section of the system.ini file. The password is encoded and is not readily decodable from the system.ini text file.

A default password is implemented automatically, however it is recommended that a specific password be defined within the system.ini file. It is important that this password be made available only to personnel requiring access to the additional diagnostic capabilities (typically only ICS Triplex Technology Ltd. personnel). If this password is lost, there is no capability of accessing these functions without reconfiguring the system.

1.8 MODULE REPLACEMENT CONFIGURATION

The system supports 3 forms of High Density I/O module replacement:

a. Companion slot (Hot-swap pair)

b. SmartSlot pair

c. Live insertion and removal

In the companion slot configuration, two adjacent module positions are coupled to provide and active and standby module pair. If it intended that the system be able to start-up (including application stop and re-start), on the primary module position, there is no requirement to define the secondary module position.

If it is intended to allow the system to start with only the secondary module position occupied, it is important that the module positions be included within the system.ini file. Identical configuration settings shall be entered for both primary and secondary module positions.

For SmartSlot pair operation, it is not possible to start-up using the “spare” module position. The spare module position need not be in the same chassis as the primary module position.

If it is intended to perform live insertion and removal without transfer to a standby module no specific configuration is required. If it is intended to start-up a system without the primary module installed in either a SmartSlot or single module live insertion and removal configuration, the “simulate” configuration option should be set. The simulate option will allow the system to start with these modules omitted, the corresponding states and values being set to their fail-safe conditions.

1. **A consistent module replacement philosophy should be used within any single system. Where mixed philosophies are used, there shall be clear indication of the repair approach applicable to each module or group of modules.**

2. **In hot-swap and SmartSlot configurations, the accuracy with both modules installed shall be within the plant required safety accuracy specification. If tighter tolerance is required, ensure that each sensor within a redundant configuration is allocated to independent modules and procedural measures are implemented to ensure that only a single module within this set of modules is paired at any instant.**

3. **If the SmartSlot module replacement is used, the system shall include provision for testing the SmartSlot linking cable. This cable shall be tested before use; the testing of this cable shall be included in the Operating and Maintenance Manual.**

4. **In hot-swap configurations, a secondary module that does not pair with the primary module in a reasonable amount of time (less than the second fault occurrence time) must be removed.**

5. **In SmartSlot configurations, a secondary module that does not pair with the primary module in a reasonable amount of time (less than the second fault occurrence time) when the SmartSlot linking cable is installed must be removed.**

1.9 INPUT AND OUTPUT FORCING

Locking and forcing of individual inputs and outputs from the IEC1131 Workbench are supported for engineering, installation and commissioning purposes. In-service, maintenance overrides for safety-related inputs and outputs should be implemented using the application program. The IEC1131 Workbench initiated locking and forcing requires:

- The TMR Processor keyswitch to be in the “Maintain“ position to make changes to the lock or force status of any point
- Access to the workbench lock & write commands, which are multi-level password protected.

A list of the currently locked points are read back from the TMR system and made available within the IEC1131 Workbench.

The TMR Processor inhibit LED will indicate when one or more I/O points are locked. The application program can determine how many points are currently locked by using the information available from the TMR Processor complex equipment; it is highly recommended that this be used to control additional status display and/or for logging purposes.

All input and output locks (and forces) can be removed using either a single function from the IEC1131 Workbench or from an edge triggered signal to the TMR Processor board within the application program. If locking is used, a safety-related input connected to an operator accessible switch shall be implemented to initiate the removal of the lock and force conditions.

It is important that the effects of forcing input and output points on the process and their safety impact are understood by any person using these facilities.

The system will allow the forced conditions to be maintained during normal operation. **When returning to normal operation it is recommended that all locked and forced points be returned to normal operation.** It is the plant operators’ responsibility to ensure that if forced conditions are present that they do not jeopardise the functional safety.

1.10 MAINTENANCE OVERRIDES

Maintenance Overrides set inputs or outputs to a defined state that can be different from the real state during safety operation. They are used during maintenance, usually to override input or output conditions in order to perform a periodic test, calibration, or repair of a module, sensor or actuator.

To correctly implement a maintenance override scheme within the TMR Controller the override, or 'bypass' logic shall be programmed within the Application Program, with a separate set of safety-related input points or variables enabling the bypass logic.

In order to accommodate maintenance overrides safely, TÜV has documented a set of principles that shall be followed. These principles are published in the document "Maintenance Override" by TÜV Süddeutschland / TÜV Product Service GmbH and TÜV Rheinland.

http://www.tuvasi.com/modr_3_d.htm

There are two basic methods now used to check safety-related peripherals connected to the TMR system:

1. Special switches connected to conventional system inputs. These inputs are used to deactivate sensors and actuators during maintenance. The maintenance condition is handled as part of the system's application program.
2. Sensors and actuators are electrically switched off during maintenance and are checked manually.

In some installations, the maintenance console may be integrated with the operator display, or maintenance may be covered by other strategies.

2. OPERATION

A safety Instrumented system (SIS) is dormant by nature, therefore in normal plant operating situations the SIS is not required and is only called upon to operate in an emergency situation.

A SIS should be designed to operate automatically and so requires no operator interaction. It is essential however that the SIS and associated field devices are maintained, to ensure they operate when required.

Before accepting ownership of a system an operator should be satisfied that the SIS has been installed and commissioned to the latest approved design documents and signed off by certifying authorities (where applicable). It is essential that document masters are maintained and fully traceable.

Modifications should not be carried out without a safety assessment and relevant approval. Modifications to a SIS, including the application, field devices and hardware, may impact the reliability and availability of the system.

Operators should know which SIS diagnostic and operational alarms are annunciated, and where they appear. For example, a system may be configured to annunciate a common status diagnostic alarm to an operator interface (SCADA/DCS etc) that requires further investigation at the panel, while all operational alarms may be individually reported on a first up basis.

Operators should be familiar with the location of the SIS documentation, spares and contact details for technical support.

3. MAINTENANCE

The operator maintenance schedule for testing the SIS, sensors and actuators should reflect the test interval used in the reliability/availability calculations.

The system should be configured to allow testing from the I/O module to the field device.

Inputs

The purpose of the override is to allow testing of the sensor without executing a trip. Inputs may be configured to have an override in the application logic which should prevent the executive action but annunciate the alarm to the operator interface. Analogue inputs should be tested over their full range.

Outputs

Output modules perform diagnostic tests as detailed in the Product descriptions.

Final element testing is usually performed by operators during scheduled plant shutdowns.

Some systems use the 8000 Series Valve monitor module to perform frequent partial valve tests while the plant is live. The cumulative data is analysed and provides details of covert failures and wear, allowing planned maintenance before a failure occurs.

Plant Maintenance

Maintenance to SIS sensors and final elements, e.g. calibration or repair/replacement while the plant is live, will require a maintenance override facility. Refer to paragraph 1.10.

SIS Housekeeping

The system should be kept clean at all times. Recommended 3 monthly maintenance should include

(1) Visually inspect the following:

1) All fuses to ensure that they are intact.

2) All 8000 Series Cabinets rack and roof fan units are working satisfactorily.

3) All terminals for tightness.

4) All modules, relays and other equipment for correct and secure location in their sockets.

5) For signs of contamination and corrosion, paying particular attention to cable joints, cable terminations, MCBs, trunking etc.

(2) Lubricate all hinges and locks.

(3) Check that the 8000 Series Cabinets are correctly ventilated and grilles are free from dust. In dusty environments, this check may be necessary more frequently.

3.1 MODULE MAINTENANCE REQUIREMENTS

There are no user-maintainable parts in any of the ***8000 Series System*** modules.

4. MODULE STATUS INDICATORS

The following sub-paragraphs detail the front panel LEDs of the ***8000 Series System*** range of modules together with their function and status.

4.1 *8000 SERIES* TMR PROCESSOR

LED	INDICATION
Healthy	Overall health of each processor slice: Steady = healthy Red flashing = slice failed.
Active	Steady green when module is in Active mode.
Standby	Steady green when module is in Standby mode. Flashing green when module has changed from Active to Standby mode.
Educated	Steady green when module is educated. Flashing green when being educated. Off when module is not educated, or application is stopped.
Run	Flashing green when module is in normal operation with full integrity. Steady green in standby. Off when the application in the Active Processor is 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 has incompatible system configuration.
System Healthy	**System health:** **Steady green = healthy** **Flashing red = system boot-up, system fault, or self-test fail, IMB error, or** *8000 Series* **I/O module error. Active/standby module failing to respond, has a slice error, channel fault, or a module is being simulated. Regent I/O module error. A module is 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 green flashing and power is switched off, then on again, the faulty slice may fail to operate again. When the *Healthy* LED is flashing red, processing is automatically switched to the standby Processor.

4.2 *8000 SERIES* TMR INTERFACE

LED	INDICATION
Healthy	Overall health of each processor slice: Steady green = healthy. Flashing green = fault.
Active	Steady green when module is in Active mode.
Standby	Steady green when module is in Standby mode.
Educated	Steady green when module is educated. Flashing green during module education. Off when module is not educated.
I/O Healthy	I/O sub-system health: Steady green = healthy Flashing Green = fault.

4.3 *8000 SERIES* TMR COMMUNICATIONS INTERFACE

LED	INDICATION
Healthy	Module health. Steady green = healthy. Flashing red = fault.
Active	Steady green when module is in Active mode.
Standby	Not used.
Educated	Not used. Set to steady green at power up.
Communications	**Six tri-coloured LEDs indicate data transfer activity on all serial communication ports and both Ethernet ports.** **The LEDs flash red when responding and green when receiving.** **The Ethernet LEDs indicate steady green in the absence of a network connection.**

4.4 *8000 SERIES* I/O MODULES

LED	**INDICATION**		
Healthy	Module health.		
	Off	=	No power applied to the module.
	Amber	=	Slice is in the start-up state (momentary after installation or power-up).
	Green	=	healthy.
	Flashing red	=	fault present on the associated slice but the slice is still operational.
	Red (momentary)	=	On installation – power applied to the associated slice.
	Red	=	The associated slice is in the fatal state. A critical fault has been detected and the slice has been disabled.
Active	Off	=	module is not in the Active state.
	Green	=	module is in the Active state.
	Flashing red	=	Module is in the shutdown state if the *Standby* LED is off.
	Flashing red	=	Module is in the fatal state if the *Standby* LED is also flashing red.
Standby	Off	=	module is not in the Standby state.
	Green	=	module is in the Standby state.
	Flashing red	=	module is in fatal state. The *Active* LED will also be flashing red..
Educated	Off	=	module is not educated.
	Green	=	module is educated.
	Flashing green	=	module is recognised by the processor but education is not complete.
Channel LED (40-off)	Off	=	open field switch (contact).
	Green	=	closed field switch (contact).
	Flashing red	=	associated channel faulty.
	Flashing green	=	associated channel input voltage out of range, i.e. either below the lowest trip threshold or above the highest.

Note: The LEDs indicating channel status may be configured to suit user requirements by implementing the procedure for configuring a System.INI file detailed in PD-8010.

5. FAULT FINDING

The ***8000 Series System*** is capable of detecting and isolating faults to module level, while its two-out-of-three voting architecture prevents faults from propagating to the system outputs. Various means are provided for directing maintenance personnel to the faulty module. Most system modules are hot-replaceable, providing continuous system operation.

The following paragraphs describe how faults are detected, annunciated, and cleared in the ***8000 Series System***. They also describe some of the basic procedures that the user should follow when diagnosing faults and repairing the ***8000 Series System***.

Note: System repair must be done promptly to ensure continued fault-tolerant operation of the ***8000 Series System***. TUV certification does not specify a minimum replacement time for faulty modules, because safety is not compromised and the faulty channel will fail-safe if further faults develop. However, it is recommended that modules that have been diagnosed as having failed should always be replaced within eight hours to maintain production (availability). Systems with a safety integrity level (SIL) rating will have a time to repair as part of the calculation, which must be followed to maintain the SIL. Modules **must** be replaced before the Second Fault Occurrence Time (the average probable time before a second fault) to avoid shutdown.

5.1 FAULT DETECTION

There are three levels of fault detection used in the ***8000 Series System***:

1. Discrepancy logic in each I/O module compares the ***8000 Series*** TMR Processor output data on each bus cycle. A fault is recorded whenever the data in one processor disagrees with the other two processors of the ***8000 Series*** TMR Processor.
2. Loopback logic on Interfaces and I/O modules is exercised by the ***8000 Series*** TMR Processors on a background basis to detect output data faults.
3. Self-test circuitry in the ***8000 Series*** TMR Processor and ***8000 Series*** TMR Interface. In addition, power supplies contain circuits for checking their output voltages.

The ***8000 Series*** TMR Processor is responsible for sorting the fault information received from the various levels and alerting the operator when system repair is required. Faults are categorised as transient or permanent based on the rate at which they occur. A separate filtering algorithm is applied to each fault type, preventing nuisance alarms from occurring on a transient fault. Figure 1 illustrates this filtering algorithm.

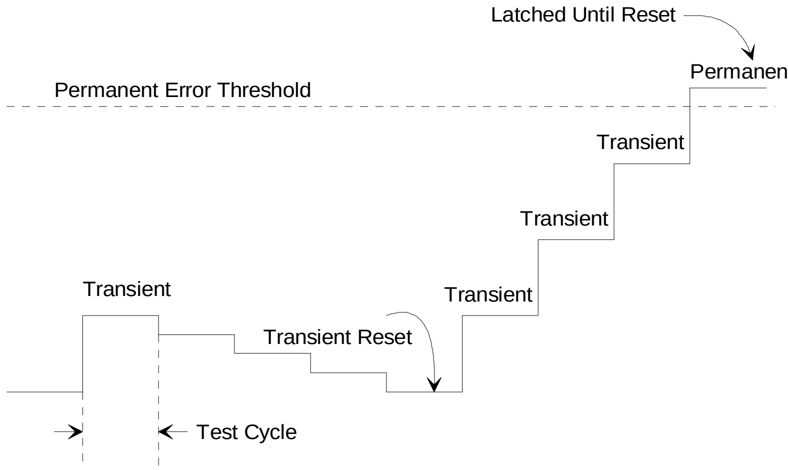

Figure 1 Fault Filtering

The system checks its fault status on a cyclic basis and if a fault is detected during that cycle, it increments a fault counter and records a transient fault. If a fault is not detected, the counter is decremented. If the counter value exceeds a threshold, a permanent fault is recorded and the counter state is held until the operator executes a reset. Whilst in the permanent state, the operator is alerted to the failure by various system annunciators. The ***8000 Series System*** allows approximately four faults in succession before a permanent fault is recorded. If a fault is detected on a ***8000 Series*** TMR Processor, a recovery process is automatically initiated to re-synchronise the module and update its memory. If the recovery process fails after the fourth attempt, no further attempts are made and the fault is annunciated.

5.2 FAULT ANNUNCIATION

The ***8000 Series System*** annunciates faults via the status LEDs fitted to the front panels of the modules.

Note: A fault indication does not necessarily mean that a module is not operational. Some faults within a module have no immediate consequence. The failure can be masked or it can be located in the test circuitry. Nevertheless, the module should be replaced and returned for repair.

8000 Series module status LEDs and their function in fault indication are detailed in paragraph 2.

5.3 FAULT FINDING TECHNIQUES

CAUTION

ALWAYS INITIATE A RESET AFTER REPLACING A MODULE. WAIT FOR THE RESET TASK TO COMPLETE (LED INDICATORS ARE RE-ENABLED) BEFORE PROCEEDING WITH FAULT FINDING.

Fault finding should always start at the ***8000 Series*** TMR Processor since it contains the first level of information regarding the operational status of the ***8000 Series System***.

After scanning the fault indicators of the system modules to locate the affected module(s), it is good practice to examine modules and connectors for proper seating, then initiate a reset to determine if the fault is permanent.

If the fault persists, then module replacement is usually the next action to take. Transient faults should be examined using the diagnostics facility to determine the frequency of occurrence and whether any corrective action is warranted.

When removing a module from an I/O sub-system, always be careful to ensure that neighbouring modules are not disturbed accidentally.

5.4 CLEARING FAULTS

Faults occurring in the ***8000 Series*** TMR Processor, ***8000 Series*** TMR Interface and ***8000 Series*** Communications Interface modules are non-latching, allowing the system to recover automatically once the fault condition has been rectified.

Faults occurring in the I/O sub-system are latched and are cleared only by first rectifying the fault, then pressing the *Reset* button on the ***8000 Series*** TMR Processor. Indication of the presence of a fault in the I/O sub-system is provided by the *System Healthy* indicator being off.

The following events take place once a reset of the system has been initiated:

1. Fault status information, indicators and fault contacts are cleared to a ‘no fault’ state. If the fault cause is transient fault rate, a single re-test (as a minimum) must be passed before returning the system to a ‘no fault’ state.

2. The *System Healthy* indicator on the ***8000 Series*** TMR Processor is lit to indicate that the reset operation is complete.

During the reset operation, all programs continue to run at their normal scan rate. There is no noticeable change in system performance and no additional vulnerability to faults. The time required to complete the reset is related directly to the processor scan time.

6. SYSTEM DIAGNOSTICS

The ***8000 Series System*** diagnostic requirements will depend upon client requirements. The recommended minimum diagnostics are included in the Software manual. Whilst some alarms indicate a fault on the module (which require replacement), others are used for analysis of the ***8000 Series System*** and indicate a fault in a secondary component.

6.1 TEMPERATURE ALARMS

Each module has dedicated monitoring points for temperature. A high temperature may indicate a faulty fan unit.

6.2 POWER SUPPLY UNIT

Redundant or N+1 configuration tolerates the loss of a power supply unit. A Power supply fault is annunciated via status contacts from the power supply to inform the operator that a power supply needs replacing.

6.3 FEED FAILURE

Should a system feed fail, and the two power feeds are isolated up to the ***8000 Series System***, all three slice LED's flash red on all modules.

7. MODULE REPLACEMENT

7.1 MODULE EJECTOR LEVERS AND KEY

When inserting a module, the ejector levers should be open and the module should be pushed into the slot using the fascia. When the module connectors have located on the backplane and field cable connectors, the module should be pushed firmly into place before closing the ejector levers.

Module ejector levers should only be opened using a 8000 Series ejector key (supplied with the ***8000 Series*** TMR Processor). This prevents damage to the ejector levers and module. The module should be handled only by the plastic case and not the connectors or pins, because the internal components are sensitive to static.

7.2 MODULE RETURNS POLICY

To enable efficient and comprehensive analysis of a module, a report detailing information that includes the conditions under which it failed should accompany the returned module. If the operator has the ‘Dumptrux’ macro, a ‘single module’ diagnostic report should be included with the returned module. The use of ‘Dumptrux’ is outside the scope of this document.

RMA: RETURNED MATERIAL FOR INVESTIGATION REPORTING FORM

Customer: …………………………….. Contact:……..…………………………………..

Unit Serial No : ……………………… Module Type: : …………………………………..

Operating condition at the time of the reported failure. Tick the relevant condition/supply information

Normal Running/Commissioning/Shutdown/System Testing/Other:

……………………………………………………………………………………………...

Description of the fault:
……………………………………………………………………………………………...
……………………………………………………………………………………………...

7.3 TMR INTERFACE MODULE REPLACEMENT

This procedure is only applicable when the TMR Interface module has failed (faulty slice) and no standby module is configured in the ***8000 Series*** Controller.

1. Insert the replacement module in the adjacent slot.
2. After the replacement module has been educated, remove the faulty module.
3. Restart the system using the ‘START APPLICATION’ procedure from the Workbench.

Note: If a catastrophic failure of the TMR Interface module has occurred, the replacement module may be fitted in the same slot as the failed module and the system re-started as described above.

7.4 ACTIVE/STANDBY CHANGEOVER

8000 Series Expander Interfaces, ***8000 Series*** Expander Processors and ***8000 Series*** TMR Interface operate in the active/standby mode when a spare module is fitted in the adjacent slot. Fitted spare modules are not required to achieve fault tolerant operation of the system.

Failures occurring in any of these modules automatically initiate an active/standby changeover, if a spare module is fitted. If no spare is fitted, insert a module of the same type, with compatible firmware and hardware, into the adjacent slot. Once the previously standby module has been educated, indicated by the *Educated* LED adopting the steady green state, the faulty module may be removed for repair. Please refer to ICS Triplex Technology for advice on compatibility.

8000 Series TMR Processor: If the system.ini file in the replacement module is identical to the installed module then a changeover occurs as above. If the replacement TMR Processor has a different system.ini file then the replacement module is educated with the system.ini file and application. At this stage, the replacement module has not yet initialised and to indicate this, the faulty module stage indicates Inhibit. The replacement module must be removed from the chassis power and then plugged back in to initialise the ‘boot’ file. When this has been done, the changeover occurs and the faulty module can be removed from the system.

7.5 COMPANION SLOT MODULE REPLACEMENT

Each I/O module in a ***8000 Series System*** may have a Companion Slot configured via a double-width I/O connector, but not necessarily occupied. This enables a faulty module to be replaced without disrupting the System.

Replacement is effected by simply inserting a working module of the same type, with compatible firmware and hardware, in the adjacent slot. The ***8000 Series*** TMR Processor automatically initiates the education of the replacement module with the appropriate data. This is indicated by the *Educated* LED flashing. When education is complete, the *Educated* LED becomes steady green, the previously active faulty module indicates ‘standby’ and the replacement module indicates ‘active’. Check that the remaining LEDs on the front panel of the replacement module are healthy (refer to section 4, Module Status Indicators). The faulty module should be removed from the System and repaired.

The ***8000 Series System*** should have a module back in the left hand (primary) slot as soon as a working module is available. Insert the new module in the left hand (primary) slot and initiate a changeover by opening the ejector levers on the right hand (companion slot) module. DO NOT REMOVE THE RIGHT HAND MODULE until the changeover has completed, the left hand module indicates ‘active’ and the right hand module indicates ‘standby’. The right hand module can now be removed.

7.6 SMARTSLOT (VERSION 2) REPLACEMENT

I/O modules in a 8000 Series system may be configured as SmartSlot, allowing modules to be replaced with another in an allocated SmartSlot. This reduces the number of slots required in a system, because a group of modules can now have one SmartSlot instead of a companion slot for every module. The cable required to connect the existing and replacement module is different for input and output modules, and so a system using SmartSlot needs at least one input SmartSlot and one output SmartSlot. A Zone Interface Module (which can be configured as both inputs and outputs) uses an output type SmartSlot cable. The SmartSlot cable is fitted to the chassis at the allocated slot and has a connector to link to the slot containing the faulty module.

SmartSlot Version 2 replacement (changeover) is effected by following the procedure detailed below.

Bridge the faulty module and SmartSlot positions by connecting the SmartSlot jumper connector to the exposed ‘C’ type connector on the rear of the faulty module I/O connector.

Insert a working module of the correct type, with compatible firmware and hardware, in the SmartSlot position. The ***8000 Series*** TMR Processor automatically initiates the education of the replacement module with the appropriate data. This is indicated by the *Educated* LED flashing. When education is complete, the *Educated* LED becomes steady green, the previously active faulty module indicates ‘standby’ and the replacement module indicates ‘active’. Check that the remaining LEDs on the front panel of the replacement module are healthy (refer to section 4, Module Status Indicators).

The faulty module should be removed from the System and repaired.

The ***8000 Series System*** should have a module back in the normal (primary) slot as soon as a working module is available. Insert the new module in the primary slot and initiate a changeover by opening the ejector levers on the SmartSlot module. DO NOT REMOVE THE SMARTSLOT MODULE until the changeover has completed, the primary module indicates ‘active’ and the SmartSlot module indicates ‘standby’. The SmartSlot module can now be removed.

Disconnect the SmartSlot connector.

8. RESTART PROCEDURE

8.1 INTRODUCTION

The procedure described below is necessary to restore the ***8000 Series System*** to full operation after a total loss of power including the loss of the incoming power supplies. The sequence is based on the assumption that the incoming power supplies have been restored after all the MCBs, contactors and isolators have been opened. It is assumed that all the application software and system INI configuration have been installed.

Note

(1) Before powering the system, ascertain the status of the plant and ensure that no danger to personnel or damage to the plant will occur.

(2) It is recommended that the *8000 Series System* should always be powered up in this sequence from cold.

(3) The last item to be powered–up will be the two Controller chassis.

8.2 POWER UP PROCEDURE

(1) Ensure that any system or devices attached to the system are ready for the powering sequence.

(2) Open the ***8000 Series System*** Cabinet doors to gain access to the incoming 240VAC system isolators. Ensure that the supply voltage is a nominal 240VAC. Close the 240VAC isolators.

(3) Close all the 240VAC MCBs. Check that both the ***8000 Series System*** Power Supply chassis are powered.

(4) Power the fan trays and roof fan assemblies, by closing the pairs of 24VDC MCBs located on the MCB Panel.

(5) Power the main ***8000 Series System*** I/O Chassis by closing the associated pairs of 24VDC MCBs located on the MCB Panel.

(6) Finally, power the ***8000 Series System*** Controller Chassis by closing the associated pairs of 24VDC MCBs located on the MCB Panel.

(7) Close the 240VAC Utilities Assembly MCBs mounted in the ***8000 Series System*** Cabinets.

(8) Ensure that the ***8000 Series System*** Engineering Workstation has power (if applicable).

8.3 8000 SERIES CABINET

(1) Press the reset pushbutton on the ***8000 Series System*** Processor Modules.

(2) Ensure that all ***8000 Series System*** Modules are healthy, and that the ***8000 Series System*** PLC is communicating.

(3) Close and lock all doors.

8.4 FINAL

(1) Ensure that all external interfaces to other systems and devices are connected and functioning correctly.

(2) Ensure that all modules are in the healthy condition relative to the state of the plant.

The ***8000 Series System*** is now ready to control and monitor trips and alarms.