

Triguard SC300E Safety Manual

Copyright © ICS Triplex Technology 1998-2005
Printed in England

Revision History

DATE	CHANGE NOTE NO	ISSUE	DESCRIPTION	INITIALS
25th Jun 98	-	A	First Issue	CJG
8th Jul 98	-	B	Updates following Review of Initial TUV Test Results	CJG
27th Jul 98	-	C	Further Update following TUV Review	CJG
18th Aug 98	-	D	Modifications Resulting from FMEA Test	CJG
6th Jan 99	-	E	Further Updates incorporating TUV Comments	CJG
13th Jan 99		F	Updates to Fault Call Bit Allocation and example networks	CJG
9th Mar 99		G	Updates incorporating TUV Comments, TUV Time Constraint times and example networks plus general updates to structure	CJG
19 th May 99		H	Updates from final TUV Review	CJG
29 th Sep 99		J	Updates from TUV Review and removal of Multiple Fault Flag shutdown from example ladder.	CJG
3 rd Nov 99		K	References to SIL 4 removed at the request of TUV.	PS
21 st Dec 99		L	Dual hot repair partners.	PS
26 th July 2000		M	New template, changed ABB to ABB Industri, Revised FALT table added appendices 4 and 5	DTW
16 th Dec 2000	released	01	Added further fault diagnostic information, corrected RTTS release info and product info	DTW
12 th Sept 2001		02	Chapter replaced by section throughout manual. 3.5.8 - I/O module dependent fault flags bit 8 updated 3.6.1 – remove analogue restriction 3.6.11 - use of triplicated watchdog with remote chassis added 4.1 - change reference to User Manual Apdx 4 – bit 4 offline modules added Apdx 5 - renumbered to 6 Apdx 5 - RTTS 8.30-007 references added Apdx 6 - 48Vdc I/O modules and termination cards added. TDOs revised. 120Vdc MDO16DNS added. Other revisions as agreed with TUV.	DTW/PS
30 th Sept 2003		03	Font change, ICS TT copyright added, ABB product references removed, IEC 61508/SIL 3 references added, F&G references added, 'polarisation keys' replaced by 'coding blocks. Definitions & Abbreviations section removed, contents added to Glossary Appendix 6 version updates. System auto-restart function described see section 3.6.4.	PS
7 th Feb 2004		04	Appendix 6, MDI32BIS part number corrected.	PS

Table of Contents

1	Glossary of Terms.....	6
2	Introduction	8
2.1	General Information.....	8
2.2	Manual Organisation.....	8
2.3	Product Introduction and Overview.....	8
2.3.1	The Triguard SC300E	8
2.3.2	SC300E Functional Overview.....	8
2.3.3	Operating System	10
2.3.4	Off-Line/Start-up Diagnostics.....	10
2.3.5	On-Line/Continuous Diagnostics.....	10
2.3.6	Verification.....	11
2.3.7	Validation	11
3	Configuration Application Design.....	12
3.1	Introduction.....	12
3.2	Assumptions.....	12
3.3	Safety Related Inputs and Outputs.....	12
3.3.1	Inputs	12
3.3.2	Outputs	15
3.4	Classification (SIL level) System Time Constraint.....	15
3.4.1	Without System Time Constraint Dual Final Elements.....	16
3.4.2	Without Time Constraint Dual Outputs	17
3.4.3	Interposing Devices.....	17
3.4.4	Systematic Software Faults.....	17
3.4.5	Process Fault Tolerant Time.....	17
3.5	Diagnostic Configuration.....	18
3.5.1	Diagnostic Message Generation.....	18
3.5.2	Printed Messages.....	18
3.5.3	Diagnostic LED's.....	18
3.5.4	Display System Diagnostics.....	18
3.5.5	Maintenance Workstations.....	18
3.5.6	Error Flags and Automatic Diagnostic Actions	18
3.5.7	Monitor flag register.....	20
3.5.8	I/O module dependant fault flags	21
3.5.9	Automatic Diagnostic Action.....	22
3.5.10	Without Time Constraint Configuration.....	22
3.5.11	With Time Constraint Configuration.....	22
3.5.12	Long Process Time Constraint System.....	22
3.5.13	Initialisation Flags.....	22
3.5.14	MPP A, MPP B, MPP C.....	22
3.5.15	Power Supply Failures.....	23
3.6	Application Software, Design, Verification and Validation.....	23
3.6.1	Non Safety Functions	23
3.6.2	Modularity and Version Control	23
3.6.3	Discretes and Register Validation	23
3.6.4	Power-Up Initialisation	23
3.6.5	Application Logic Verification	23
3.6.6	Application Logic Validation.....	24
3.6.7	Start-up Overrides	24
3.6.8	System Acceptance Test.....	24
3.6.9	Application Software Documentation.....	24
3.6.10	Application Logic Driven External Triplicated Watchdog Timer	24
3.6.11	Use of Triplicated Watchdog Timer with Remote Chassis.....	24
3.7	TriBuild, Network Examples	25
3.8	Environmental Functionality	25
3.9	Security	25
3.10	System Power Supplies.....	25
3.11	Field Sensors and Final Elements.....	25

3.11.1	Field Power Supplies	25
3.11.2	Field Power Distribution	25
3.11.3	Field Power Diagnostics	25
4	Installation And Commissioning.....	26
4.1	Introduction	26
4.2	Site Planning and Environment	26
4.3	Process Field Connection.....	26
4.4	Systems Start-up and Shutdown Procedures	26
4.4.1	General Description - Start-up Procedure	26
4.4.2	General Description - Shutdown Procedure.....	27
4.4.3	Application Changes During Commissioning	27
4.4.4	Site Acceptance Test Validation	27
4.4.5	Permits to Work.....	27
4.4.6	Module Slot Security.....	27
5	Operations	28
5.1	Introduction.....	28
5.2	Training.....	28
5.3	System Start-up.....	28
5.3.1	Process Loading and Start-up.....	28
5.4	System Operation.....	28
5.4.1	Maintenance Alarm	28
5.4.2	Maintenance Actions.....	28
5.4.3	Process Trips and Events.....	29
5.4.4	Maintenance Engineering Station	29
5.5	System Shutdown	29
5.5.1	Process Shutdown.....	29
5.5.2	Triguard SC300E System Shutdown	29
6	Maintenance And Modifications.....	30
6.1	Introduction.....	30
6.2	Routine Maintenance	30
6.2.1	System Verification	30
6.2.2	Diagnostic Alarms and Messages	30
6.2.3	Module Change-Out.....	31
6.2.4	Sequence of Repair.....	32
6.2.5	System Time Constraints.....	32
6.2.6	Life Cycle Proof Test	33
6.2.7	Maintenance Overrides.....	33
6.2.8	Minor Modifications.....	33
6.2.9	HAZOPS	34
6.2.10	Design	34
6.2.11	Verification and Validation	34
6.2.12	Installation and Commissioning	34
6.2.13	Acceptance Test Validation.....	34
6.2.14	Personnel.....	34
6.3	Training.....	34
6.4	Security	34
6.5	Failure Reporting	34
6.6	Maintenance Completion.....	35
7	De-Commissioning.....	36
7.1	Introduction.....	36
7.2	Final Process Shutdown.....	36
7.3	Dismantling and Removal	36
7.3.1	Electronic and Electrical Modules	36
7.3.2	Mechanical Items	36
7.3.3	Safety Precautions	36
8	Appendix 1 - Safety Networks.....	37

9	Appendix 2 - Time Constraint Table (Low Demand of operation)	50
9.1	Admissible Repair Times in hours for Low Demand Mode of Operation.....	50
10	Appendix 3 - Approved RTTS Versions	51
11	Appendix 4 - RTTS versions 8.30-005 and later versions	52
11.1	System Error Flags for RTTS version 8.30-005 and later versions.....	52
11.2	MHB44IND 4 channels pulse input and 4 channel analogue output module.	52
11.3	MAO04IND 4 channel analogue output module.....	53
11.4	System identification.....	53
11.4.1	SC300E RTTS 8.30-005.....	53
11.4.2	SC300E RTTS 8.30-006.....	53
12	Appendix 5 – RTTS 8.30-007 and 008	54
12.1	System Identification RTTS 8.30-007.....	54
12.2	Change History	54
12.3	System Identification RTTS 8.30-008.....	54
12.4	Change History	54
13	Appendix 6 - TUV Approved Part Numbers and Revisions	55
13.1	Hardware Approvals.....	55
13.2	Software Approvals.....	59

Table of Figures

Figure 1	System Overview.....	10
Figure 2	Current to Voltage Conversion	14
Figure 3	Dual Final Elements.....	16
Figure 4	Dual outputs to single final element	17

Table of Tables

Table 1	FALT Error Flags (RTTS 8.30 versions 001 – 003).....	19
Table 2	Monitor Flag Register	21
Table 3	Digital Output Fault Flags.....	21
Table 4	Piano and Analogue Fault Flags.....	22
Table 5	System Alarms	22
Table 6	FALT flags RTTS 8.30-005 and later	52

1 Glossary of Terms

1oo2	One out of two voting
2oo2	Two out of two voting
2oo3	Two out of three voting
3-2-1	Three to two to one processor degradation
3-2-0	Three to two to zero processor degradation
A,B or C	System channel reference
ac	alternating current
BSI	British Standards Institute
CE	Indicates compliance with applicable European Community directives
CI	Common Interface (a daughter board fitted to I/O modules).
dc	direct current
EMC	Electro Magnetic Compatibility
EPROM	Erasable Programmable Read Only Memory
ESD	Emergency Shutdown
F&G	Fire and Gas
FAT	Factory Acceptance Test
FPGA	Field Programmable Gate Array
GTZ	Go To Zero
HW	Hardware
id	identity
I/O	Input and/or Output
IEC	International Electrotechnical Commission
ISO	International Standards Organisation
LED	Light Emitting Diode
LFD	Latent Fault Detection
MBB	Bus Buffer Interface module
MDR	Mandatory Design Review
MPP	Main Processor
MTTR	Mean Time To Repair
PAC	AC Power Supply for a Triguard system
PID	Proportional, Integral and Derivative - process control signals
PLC	Programmable Logic Controller
PSU	Power Supply Unit
PVCS	Product Version Control Specification
QA	Quality Assurance
QM	Quality Management
RAM	Random Access Memory
ROM	Read Only Memory
RS232C	Serial binary data exchange standard
RTTS	Real Time Task Supervisor (Main Processors operating system.)
SAT	Site Acceptance Test
SIFT	Software Implemented Fault Tolerance
SS	Standard Specification
SW	Software
System channel	One third of a triplicated circuit
THR	Hot Repair Adapter Card
TMR	Triple Modular Redundancy
TriBuild	Software application programming package for SC300E

TÜV	Technischer Überwachungs Verein, translates to Technical Supervisory Association, of Germany
TWD	Triplicated Watchdog
UL	Underwriters Laboratories
V&V	Verification and Validation
WI	Work Instruction

2 Introduction

2.1 General Information

This Safety Manual provides the information necessary to safely configure, install, operate, maintain and de-commission Triguard SC300E Safety Controllers certified for safety applications.

It should be recognised that this manual applies to all safety critical functions only. Where functions apply to monitoring, indication only or non safety applications this manual does not necessarily apply.

On all systems relating to safety it is first necessary to decide which I/O points are directly related to the safety functions. These will normally include all inputs and outputs documented on the "cause and effect charts" or "fault schedules", but may include other monitoring or control points. It is the responsibility of the System Designer to enquire if any additional points are safety related.

By following the guidance in this manual, the user will be assured that his Triguard SC300E Safety System will be configured, installed, commissioned, operated and maintained with safety first as the prime objective. This manual however can give no assurance that the basic safety specifications (cause and effects/fault schedule) are correct.

This manual is restricted to safety aspects of the functions covered and does not remove the requirements to follow the guidance in SC300E User Manual 008-5197.

2.2 Manual Organisation

The manual is structured following the introduction section to follow the safety aspects of the Life Cycle model of the Triguard SC300E Programmable Safety Systems. Sections are therefore provided on the safety aspects of Design and Configuration, Installation and Commissioning, Operation, Maintenance and De-Commissioning.

2.3 Product Introduction and Overview

2.3.1 The Triguard SC300E

The SC300E has been designed as a cost effective, fault tolerant control system suitable for use in industrial situations where the control system's reliability, availability and predictable performance is of paramount importance. The Triguard SC300E is certified for use in safety applications, such as process and emergency shutdown. For fire and gas applications refer to the Safety Manual SS 0799.

The two key components of the Triguard SC300E, that permit system availability's in excess of 99.999%, (about 1 hour downtime in 11 years) to be realised, are as follows. System availability is calculated using MIL 217F failure rates and a given MTTR of typically 4 hours. Lengthening or shortening the MTTR will decrease or increase the system availability respectively.

- Triple Modular Redundant architecture - TMR
- Software Implemented Fault Tolerance - SIFT

2.3.2 SC300E Functional Overview

A Triguard SC300E system has a fully triplicated architecture from input modules to output modules. All Triguard SC300E input and output modules interface to three isolated I/O communications buses, each being controlled by one of the three processor modules.

At the input modules, field signals are filtered and then split, via isolating circuitry, into three identical, signal processing paths. Each path is controlled by a microcontroller that co-ordinates signal path processing, testing and signal status reporting to its respective processor, via one of the triplicated I/O communications buses.

Each of the processors communicates with its neighbours via read only, serial communications links. The processors synchronise at least once per application logic execution cycle, and each reads the input, output and diagnostic status of its neighbours. Each processor correlates and corrects its memory image of the current state of the system using a 2-oo-3 software vote, logging any discrepancies found in a local diagnostic history table.

Each processor then executes its programmed application logic and sets its respective outputs, via the I/O communications bus, to the required state.

Commanded output states are received by an output module's microcontrollers which, using 2-oo-3 hardware voters, set the outputs to the field. Any discrepancy between a commanded output state and the field output is detected by the microcontrollers and reported to the appropriate processor.

All input and output modules can be configured to use a hot spare partner module. In the event of a fault on the main I/O module its duty can be taken over by the hot spare partner, allowing repairs to be effected.

In maximum configuration a single SC300E system can support a main chassis and 14 extension or remote chassis. Each chassis can be populated with 10 modules each containing up to 32 I/O channels, however, for safety configurations all outputs are configured for dual slot hot repair. Input modules may be configured for single slot hot repair only where the input configuration or process safety time allows.

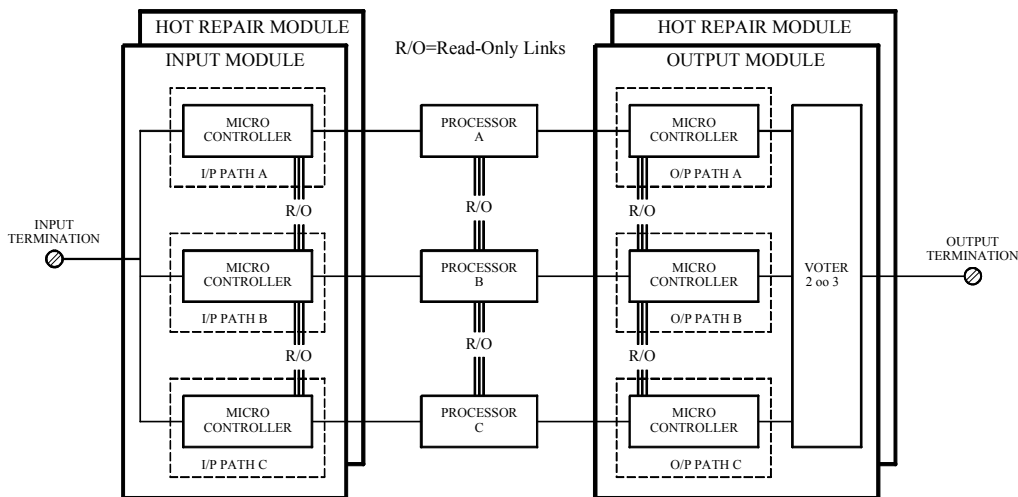


Figure 1 System Overview

2.3.3 Operating System

The SC300E's Real Time Task Supervisor (RTTS) is a derivative of the CS300 series operating system that has accrued over 10 million operational hours.

The RTTS is transparent to a user - an SC300E system is programmed like any standard industrial PLC, and controls the offline/start-up and online/continuous diagnostics.

2.3.4 Off-Line/Start-up Diagnostics

When an SC300E's processors are first powered up, the following diagnostic routines are executed: -

- initialisation of all RAM
- memory configuration and size checks
- RTTS and application logic copied to RAM
- all program checksums recalculated and checked
- configuration and checksums of neighbouring processors read and confirmed
- initialisation of synchronisation registers
- synchronisation registers of neighbouring processors read and verified

A processor will then pause, waiting for the other two processors to complete their start-up diagnostics.

At power up an SC300E system must have three healthy processors, otherwise the start-up diagnostics will prevent execution of the system application logic. The RTTS permits an SC300E system to operate 3-2-0 i.e. a system will continue to operate with one failed processor. For ESD safety configurations output modules are configured to de-energise their outputs when the second processor fails.

Replacement processors can be brought online using a warm start command. Warm start commands can be issued from a TriBuild workstation or by use of application logic. A newly installed processor will execute its start-up diagnostics, monitor the running processors' synchronisation registers and await a warm start command. At this point checksums will be confirmed and the new processor acquires I/O data tables and the application program from its neighbours and commences execution of its application logic.

2.3.5 On-Line/Continuous Diagnostics

All memory reads and writes are automatically checked for errors by the processors' error checking and correcting circuitry. Single memory errors are detected and corrected, all multiple errors are flagged.

SIFT votes the data tables between the processors 2oo3, any errors being logged and corrected by the processors during their 'read neighbour's data' cycle.

Corrected memory errors are logged in diagnostic history tables. These tables can be accessed by application logic functions and be used to generate system alarms. If multiple memory errors on a single process are detected the processor will be halted and its watchdog tripped.

The I/O 'Hot Repair' task regularly scans all configured I/O slots to determine their status. All I/O modules have identity type registers that allow the hot repair task to confirm the status of all fitted modules: -

- correct module type fitted and online, healthy
- correct module type fitted and offline, healthy
- module type xxx missing
- incorrect module fitted xxx, should be yyy

For further information regarding the RTTS please refer to the 'TriBuild Software Manual 008-5206'.

For a full description of Triguard SC300E modules refer to the Triguard SC300E Product and Application Guide (008-5112) and the relevant Module User Manuals.

2.3.6 Verification

The proving of a part of the system that it meets its specification and only its specification. Verification can be on a small part of the system such as a single application function, or up to the complete system with only simulated field devices and other peripherals. For example at 'The Factory Acceptance Test'.

2.3.7 Validation

The proving of the complete installed safety system includes all field devices and interfaces. For example at 'The Site Acceptance Test'.

3 Configuration Application Design

3.1 Introduction

This section provides the guidelines that must be followed if certification to DIN VDE 0801 AK 6 / IEC 61508 SIL 3 is to be maintained. The guideline deals only with the Triguard SC300E Safety PLC and its implementation into a Safety System. It does not remove the responsibility of the Systems Designer to ensure that all other analysis and design processes have been completed correctly.

This section covers the design and configuration of a Safety System based on the Triguard SC300E Product up to and including the factory acceptance stage.

3.2 Assumptions

The following assumptions have been made in this section.

The system design/integration company is operating accredited quality procedures for the design and manufacture of Software based Safety Systems to the standard of ISO 9001, TOPS or equivalent or higher standard and has received training on Triguard SC300E system integration.

That all earlier life cycle parts of the design phase have been completed correctly including Hazops and Safety Loop Systems Integrity Level (Safety Classification) Requirements

That the specified plant input and output configuration fully meets the required Safety Classification (Safety Integrity Level) Selections (eg for Safety Classification AK6 (Safety Integrity Level 3) Loops at least 2 independent final element paths are established).

That the Cause and Effect, Fault Schedule, Function Block Diagrams or other primary design information is correct.

That the process safety times have been defined.

That the process safety time constraint has been defined.

3.3 Safety Related Inputs and Outputs

The Safety Loops, Cause and Effect Charts or other design data will define which loops are to be considered as Safety Loops. All inputs and outputs associated with Safety Loops must follow the design guidelines laid out in this section.

All Modules must be configured for 320 fail safe operation.

All output modules associated with Safety Loops must be configured with adjacent hot repair partner slots. The hot repair partners for output modules must not be fitted during normal operation.

If the process time constraint is less than 30 seconds, or only single sensors are provided for process measurement, then all input modules associated with safety loops must also be configured with adjacent hot repair partner slots.

3.3.1 Inputs

Safety inputs to a Safety System will be either Normally Energised Digital Inputs (De-Energise to Trip) or Analogue Inputs.

3.3.1.1 Digital Inputs

De-energise to trip inputs (usually termed fail-safe) will be used for all safety digital inputs. The number of safety monitoring signals required for each safety parameter will depend primarily on the safety integrity level (safety classification) required to be achieved, the 100% proof test cycle required and the level of diagnostics available from the field device.

All safety digital inputs will be wired to a Digital Input Termination Card. Where the safety integrity level requires that more than one field sensor monitoring a safety parameter, each of these sensors should be, where practical, wired to separate Termination Cards. The Simplex part of the termination card (eg fuses) must be considered for reliability analysis as part of the field loop.

The Termination Card will be connected to the Triguard SC300E Input Module via a standard system cable which connects to the socket on the appropriate Hot Repair Adapter Card (THR) or chassis slot.

Through the hot repair adapter card, where required, and the chassis backplane connector the input signal is connected to the configured digital input slot position where a Digital Input Module would be located.

All the chassis slots and, where required, its hot repair partner slots configured for the Digital Input Module must also have the coding blocks fitted and configured for this type of module as specified in the Module and Chassis Users Manuals.

Where the safety integrity level requires that separate sensors are used to monitor the same safety parameters they should be configured to separate Digital Input Modules where practical.

3.3.1.2 Analogue Inputs

Analogue transmitters are used to monitor safety parameters and inherently provide an increased level of diagnostics with respect to a simple fail-safe digital input. Analogue signals always provide values within a set operating range. For safety related transmitters this should be 4-20mA or 1-5 volts allowing for fault indication below say 3mA (0.75V) and 20mA (5V). If over-range detection is required a 0-10V input module must be used. All monitored faults from the analogue signals must be used by the application software to produce fail-safe results (eg failed transmitter demands a shutdown).

The number of analogue transmitters used to monitor a safety parameter will be dependent on the system integrity level (safety classification) requirement of the loop, the 100% proof test cycle of the loop and the level of diagnostics available from the transmitter.

The field analogue signal is wired to the Analogue Input Termination Card. Where the safety integrity levels require that more than one transmitter be used to monitor a safety parameter, then the additional analogue input signals should be wired to separate Termination Cards where practical. The Simplex circuitry on the termination card must be considered for reliability as part of the transmitter loop (eg fuses and monitoring resistors where fitted). Refer to Figure 2.

The signal is connected from the termination card to the Triguard SC300E input module via a standard system cable, which connects to the socket on the appropriate Hot Repair Adapter Card (THR) or chassis connector.

Through the Hot Repair Adapter Card, where required, and the chassis backplane connector the input signal is connected to the appropriate configured analogue input module slot position, where an appropriate Analogue Input Module would be located.

All the chassis slot and, where required, their hot repair partner slots configured for the Analogue module must also have the coding blocks fitted and configured for this type of module as specified in the Module and Chassis User Manuals.

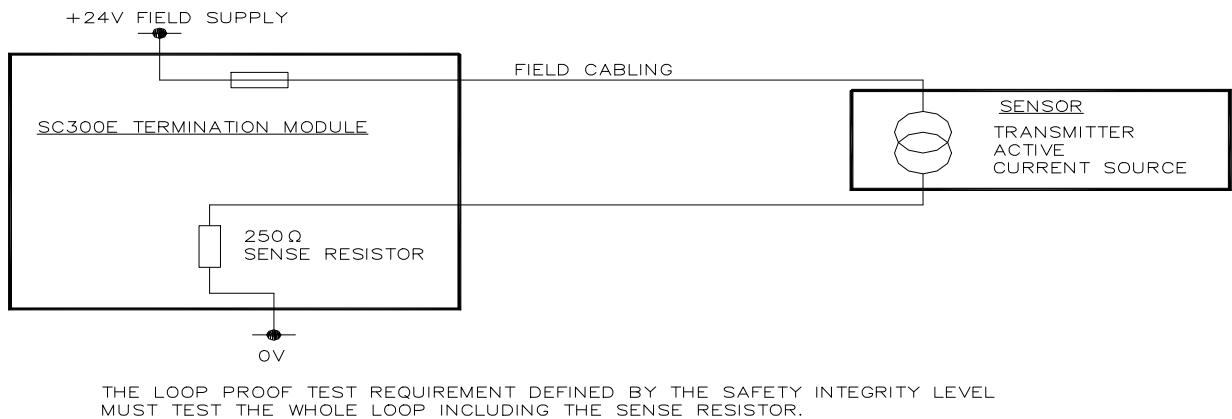


Figure 2 Current to Voltage Conversion

Where separate transmitters are used to monitor the same safety parameters to meet increased integrity levels these should be configured to separate Analogue Input Modules where practical.

Switch inputs with end of line and series line-monitoring resistors fitted may be connected as analogue inputs. These line-monitored inputs provide increased diagnostic information to the safety system giving discrete analogue values (step changes) for open circuit, switch open, switch closed and short circuit conditions.

3.3.1.3 Fail Safe Analogue Processing

For each Analogue Input variable received by the system three values are generated, one from each channel. Under normal operation (transparent to the application) a mid-value selection algorithm is used selecting the middle value (assuming all three values are within the health window) to be passed on to the application. It is this mid-value that the user operates on within the application, all three processing channels now using this selected mid-value.

When one of the three analogue channel values presented to the processors falls outside of the health window the processors flag it as bad by converting it to a negative number. If now the two remaining values diverge by more than the health window these are also flagged as bad by converting them to negative numbers. The effect is to present to the application a negative value when 2 or more channels are bad.

The application, by use of either the analogue processing module (available in USR3) or simple comparators, can provide a bad/safe discrete for each analogue value. An example network using comparators is given in Network 7 of the example networks. Network 6 shows the same functionality using USR3 (See Appendix 1).

When large numbers of Analogue Inputs are to be processed, USR3 should be used to effectively monitor faults within the analogue loops. This is accomplished by configuring the Analogue Test Database in the TriBuild System Configuration Special Function Configuration.

This configuration provides for each analogue variable an array of discrettes for channel faults, open and short circuit faults, as well as defining a global fault bit and the test parameters. Both open and short circuit faults values should be configured.

3.3.2 Outputs

The standard configuration for ESD Safety System outputs is to provide digital outputs only, which are configured for de-energise to trip (3-2-0 GTZ again fail to safe).

3.3.2.1 De-Energise to Trip Outputs

All safety related outputs will be from the Digital Output Module. Each module must be configured with a hot repair partner slot to allow bump-less hot repair to be accomplished.

The Output Module provides a fully tested six-element switch voting circuit for each individual output.

Where the safety integrity level (safety classification) requirements of a safety loop requires two or more final elements to be available for shutdown purpose, then each final elements should be driven from a separate Digital Output Module and Termination Card, where practical.

The shutdown signal is connected from the Output Module through the chassis backplane, the hot repair adapter card and the system cable to the Termination Card where the field wiring is connected.

The simplex part of the termination module (eg fuses) must be considered as part of the field loop for reliability analysis.

3.3.2.2 Multiple Input / Output Safety Configuration

Where the safety integrity level requires multiple sensors and final elements from a safety loop, then these configurations will be as follows.

3.3.2.3 Dual Sensors

These will be voted by the application logic in a 1oo2 manner such that either sensor providing an alarm status requires a shutdown.

Where the sensor diagnostics provide fault status then the safety loop may revert to a 1oo1 voting on the good sensor for the time constraint of the sensor's safety loop. At the termination of this time constraint the loop will demand a shutdown.

A single remaining sensor going into fault will demand an immediate shutdown.

3.3.2.4 Triplicated Sensors

These will be voted on a 2oo3 basis by the application logic, however, once a sensor has been voted as bad, the voting logic will revert to a 1oo2 vote on the remaining two sensors following the strategy determined for dual sensors.

3.3.2.5 Dual Final Elements

These are to be configured in a 1oo2 manner such that either output requires a shutdown.

3.3.2.6 Hot Repair Adapters

Wherever dual slot hot repair facilities are required, the hot repair adapter boards must be fitted on the chassis backplane.

3.4 Classification (SIL level) System Time Constraint

The Triguard SC300E Safety PLC is a fault tolerant system that inherently tolerates and reports a first major fault (for example a processor failure).

The system diagnostics of a digital output module are not fully available after a first fault is found on the module. The time allowed to repair this module before a shutdown to the safe state is required is the system time constraint.

The Triguard SC300E System may be configured with or without time constraint dependent on the safety output configurations used.

In systems configured with single outputs and final elements, then a time constraint will apply.

The time constraint has been conservatively calculated by TUV dependent on the SIL level (low demand) and based on worst case of all outputs used.

- Time constraint for SIL 3 systems is 2353 hours
- Time constraint for SIL 2 systems is 7440 hours
- Time constraint for SIL 1 systems is 23528 hours

Time constraint may be extended if less than 32 outputs are safety related, for extended time constraint values refer to the table Appendix 2.

3.4.1 Without System Time Constraint Dual Final Elements

In AK6 (SIL 3) classified safety loops it is probable that the safety loop final element has at least two possible operational paths (Figure 3 shows a typical configuration).

Providing each final element is driven from a separate SC300E digital output on separate digital output modules, the system will have no time constraint.

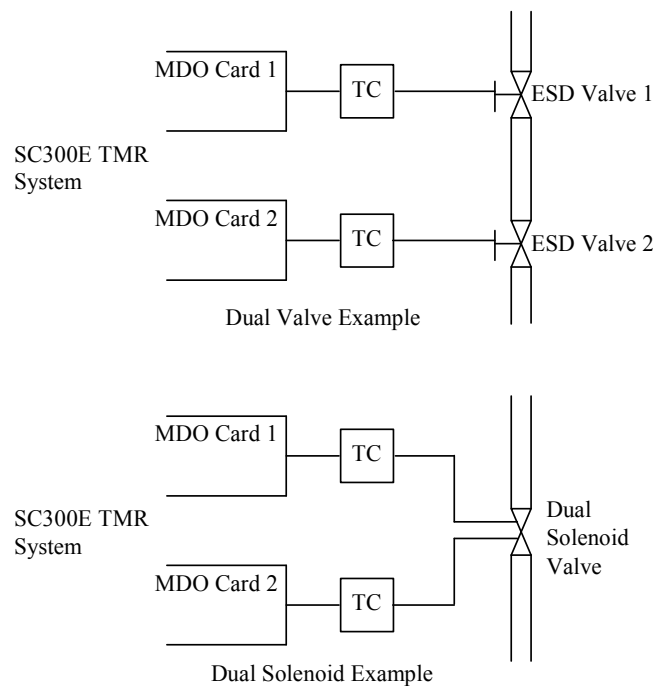


Figure 3 Dual Final Elements

3.4.2 Without Time Constraint Dual Outputs

In AK6 (SIL 3) classified safety loops with only one final element, then the final element must be controlled from two digital output channels on separate digital output modules. (Figure 4 shows a typical configuration).

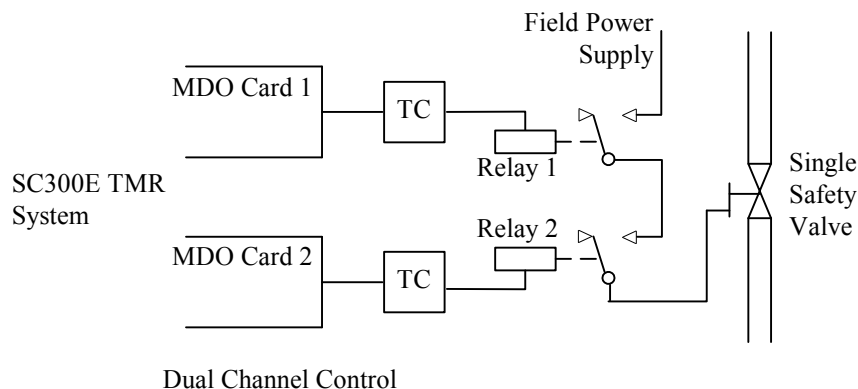


Figure 4 Dual outputs to single final element

3.4.3 Interposing Devices

The use of interposing devices such as IS barriers and relays are not part of the certified PLC system and must be considered for reliability as part of the field loop. However, the following is recommended.

IS barriers should be certified (Germany PTB / BASEEFA / SEV) and compatible with both the Triguard SC300E I/O module and the field device. Where barriers are mounted on manufacturer's barrier termination card, the PLC certification ends at the barrier termination card safe area connection.

Simplex Interposing relays should be configured with 2-pole isolation in order to eliminate simplex fail to danger modes.

Where interposing relays operation is only to be monitored by contact feedback from the relay these should be safety type relays.

It is the responsibility of the system designer to advise the end user of all such devices that are included within the safety systems scope of supply in order for the end user to evaluate their configuration and suitability for the complete safety loop.

3.4.4 Systematic Software Faults

To provide further tolerance to systematic design and application software faults, for example continuous loops, the application TMR watchdog is incorporated. An example of its application is shown in the example networks.

3.4.5 Process Fault Tolerant Time

The configuration must ensure that the specified process fault tolerance time must be equal or greater than twice the PLC cycle time plus the field equipment switching time. The PLC cycle time can be estimated from the scan rate data estimator (Triguard SC300E Scan Rate Estimator SS 0730) and may be confirmed by monitoring the three registers available for displaying: -

R1980	-	Scan Rate Set in centiseconds
R1981	-	Scan Rate Time in centiseconds
R1982	-	Scan Rate Used in centiseconds

For full details refer to the TriBuild Help Facility.

3.5 Diagnostic Configuration

The Triguard SC300E Fault Tolerant Safety PLC provides an extremely high level of hardware fault diagnostics. All diagnostic errors found initiate a change in state in the Fault Register. It is therefore mandatory that the Fault Call Module be activated in one of the diagnostic networks to provide access to system level diagnostics.

3.5.1 Diagnostic Message Generation

The activation of the Fault Call when an error is found must be used to provide a diagnostic maintenance message to the operator, to allow repair actions to be taken. Diagnostic messages can be provided in a number of acceptable formats, eg Printed Messages, Operator Alarms, Diagnostic LED Alarms and Diagnostic Alarm Mimics on Operator Stations. A minimum of one digital output must be configured to give a fail-safe output to ensure that the operator/maintenance is made aware that there is a problem with the system that needs action.

A combination of methods is usually utilised to provide the maintainer with diagnostic information and the operator with alarm and status information.

For information on the Triguard error bits refer to the Triguard User Help facility.

3.5.2 Printed Messages

The triplicated database can contain a number of printed messages that can be triggered by events such as diagnostic alarms and plant alarms. The printed messages database is prepared by a Systems Designer linking the discrete, to which the event is to be referenced, to the alarm diagnostic message to be printed. The message database is compiled and loaded as part of the load module.

3.5.3 Diagnostic LED's

As all diagnostic information exists as discrettes within the database, these can be utilised to drive outputs directly to light panel mounted LED's for example. It is also practical to utilise the Dual Serial Multiplexer System TM117DMX to drive LED's for alarms. The TM117DMX is not approved for safety critical signals.

3.5.4 Display System Diagnostics

In systems that are provided with Operator Workstations for graphical alarm information (such as TriCommand), diagnostic display mimics can be generated allowing VDU diagnostic alarm displays of the diagnostic discrettes. These operator stations are not normally fault tolerant and as such are not considered as part of the safety system.

3.5.5 Maintenance Workstations

The Password Protected Maintenance Workstation is used to display the diagnostic and history tables in a snapshot manner, it also provides detailed diagnostic information on I/O module and I/O channel errors. During operation it is not necessary to have the maintenance workstation continuously attached to an operating Triguard SC300E PLC. When maintenance actions have been completed the TriBuild Workstation should be disconnected from the operating SC300E PLC.

3.5.6 Error Flags and Automatic Diagnostic Actions

The diagnostics available through the TriBuild Workstation are extremely comprehensive and detailed down to channel level. A summary of these diagnostics is made available to the user by the use of the "Fault Call", which provides a voted set of diagnostic flags.

The fault/error flags will be located in the Register specified by the user in the "Fault Call" and are defined as follows (for RTTS 8.3-005/006 see appendix 4): -please use table for RTTS 8.3-001 to 003

Bit	Reference	Description
0	History	Entry in history table - errors logged relating to processors and communications
1	Data/Voting	2003 voting error – voting discrepancies encountered and logged by the processors during I/O scanning
2	LFD	latent fault detection of failed on or failed off signal paths – monitor and fault bits set depending on fault type and location
3	Monitor	Initialisation error – bits are set in the fault or monitor registers
4	INIT	System initialisation error – modules referenced in the table of operations are missing. Either a single slot module or both modules missing in a dual slot hot repair partnership.
5	MPP A	Processor A failure – out of synchronisation
6	MPP B	Processor B failure – out of synchronisation
7	MPP C	Processor C failure – out of synchronisation
8	MPP A power	Processor A loss of power – fuse or PSU
9	MPP B power	Processor B loss of power – fuse or PSU
10	MPP C power	Processor C loss of power – fuse or PSU
11	MPP low Battery	Memory battery - low charge on one or more of the processor's batteries
12	Off-line module	Single slot repair - module off-line – should be on-line.
13	Digital Output	Fault on any digital output module(s)
14	Multiple fault	Multiple faults on a module
15	Reserved	

Table 1 FALT Error Flags (RTTS 8.30 versions 001 – 003)

The error flags should be used to give primary indication to the operator/maintainer that a fault exists within the system. In addition to the error flags the chassis system power supply fault contacts should also be wired to at least one digital input channel and used for system power supply fault reporting. On the majority of systems other external fault indications would be wired to digital input channels to provide maintenance alerts (eg cabinet temperature, field power supply failure, loop fuse failure etc).

3.5.6.1 Bits 0 - History

Entries in the system History table – the errors in the history table are those related to the processors and communications areas.

3.5.6.2 Bit 1 - Data/Vote

Data (vote) entries – these errors are due to voting discrepancies encountered during the I/O scanning. This bit is set by the main processors detecting errors and not the I/O modules and therefore does not result directly in any other monitor/fault bits being set in the exception tables.

3.5.6.3 Bit 2 - LFD

LFD entries – these errors are due to latent fault testing of the I/O modules. LFD testing is done on each I/O module in turn on a 20 second rotating basis. Since genuine LFD errors are detected by the I/O module they will result in the I/O module health lamp being turned off and other bits in the monitor/fault flags being set eg if system channel A has a fault then the monitor flag bit 1000h would be set. It should be noted that LFD testing is not carried out on an output module that is detected as not being healthy. However, LFD continues on input modules after the first fault has been detected. LFD errors can also be generated by field faults on output modules only, example: open circuit field loops.

Note: prior to RTTS version 8.30-003, the LFD cycle was 50 seconds.

3.5.6.4 Bit 3 - Monitor

Monitor entries – this bit indicates that there are at least one or more bits set in the monitor/fault flag registers. There are two registers that contain this data – a monitor register and a fault register.

3.5.6.5 Bit 4 - INIT

Initialisation errors (missing modules) – this bit indicates that modules configured to be present in the table of operations at build time are not actually in the system. Dual slot hot-repair partners are of course not required to be present.

3.5.6.6 Bit 5 - MPPA

MPP 1 out of synchronisation (halted).

3.5.6.7 Bit 6 - MPP B

MPP 2 out of synchronisation (halted).

3.5.6.8 Bit 7 - MPP C

MPP 3 out of synchronisation (halted).

3.5.6.9 Bit 8 - A Power

MPP 1 Power health – this bit indicates that there is a problem with one of the power feeds into the processor – either fuse blown or possibly no chassis PSU fitted.

3.5.6.10 Bit 9 - B Power

MPP 2 Power health – this bit indicates that there is a problem with one of the power feeds into the processor – either fuse blown or possibly no chassis PSU fitted.

3.5.6.11 Bit 10 - C Power

MPP 3 Power health – this bit indicates that there is a problem with one of the power feeds into the processor – either fuse blown or possibly no chassis PSU fitted.

3.5.6.12 Bit 11 – Battery Low

Global MPP battery low, one or more processors batteries have low charge or are missing.

3.5.6.13 Bit 12 - Single Slot Off-line

Module off-line – this bit indicates that there is at least one module, which is off-line although it should be on-line. This will become active if a single slot hot repair module is taken off-line.

3.5.6.14 Bit 13 - Digital Output fault

Digital output error – this bit indicates that there is an error with at least one digital output module in the system.

3.5.6.15 Bit 14 - Multiple Fault

Module multiple fault – this bit indicates that an MPP is out of sync and at least one other monitor fault flag or I/O module dependant fault flag register bit is set.

3.5.6.16 Bit 15 - Reserved

Reserved for future use.

3.5.7 Monitor flag register

The setting of bit 3 in the 'FALT' call register above results from any bit being set in the 16 bit monitor flag register. These bits are set in the shared RAM on the common Interface by the microcontroller and read by the main processors.

Bit	Reference	Description
0	Microcontroller	Microcontroller A watchdog timer timed out

	health A	
1	Microcontroller health B	Microcontroller B watchdog timer timed out
2	Microcontroller health C	Microcontroller C watchdog timer timed out
3	MPP A health	MPP A watchdog timer timed out
4	MPP B health	MPP B watchdog timer timed out
5	MPP C health	MPP C watchdog timer timed out
6	Power fault	Any power fault on the module
7	Reserved	
8	Reserved	
9	Reserved	
10	Reserved	
11	Reserved	
12	Programmatic Health – A	Health Lamp turned off by microcontroller A
13	Programmatic Health – B	Health Lamp turned off by microcontroller B
14	Programmatic Health – C	Health Lamp turned off by microcontroller C
15	Reserved	

Table 2 Monitor Flag Register

3.5.8 I/O module dependant fault flags

The 16 bit fault flag register has a format dependant on the I/O module type. Currently only the DO and Piano and Analogue output modules are supported.

Bit	Description
0	Logic Supply A power fail fault
1	Logic Supply B power fail fault
2	Logic Supply C power fail fault
3	Field Supply A power fail fault
4	Field Supply B power fail fault
5	Field Supply C power fail fault
6	Bias Supply 1 power fail fault
7	Bias Supply 2 power fail fault
8	Logic supply power fail fault
9	Reserved
10	Reserved
11	Drive Supply A power fail fault
12	Drive Supply B power fail fault
13	Drive Supply C power fail fault
14	Field supply power fail fault
15	Over temperature fault (not currently implemented in hardware)

Table 3 Digital Output Fault Flags

Bit	Description
0	Logic Supply A power fail fault
1	Logic Supply B power fail fault
2	Logic Supply C power fail fault
3	Reserved
4	Reserved
5	Reserved
6	Field power fail fault
7	Output discrepancy error

8	Reserved
9	Reserved
10	Reserved
11	Reserved
12	Reserved
13	Reserved
14	Reserved
15	Reserved

Table 4 Piano and Analogue Fault Flags

The following alarm contacts are available and can be wired into the system for use by the application logic.

Power supply fault	2 off, any system or field power supply
System cabinet over-temperature	Cabinet high temperature \ ventilation alarm, if fitted.
Fuse failure	Any fuse failure, grouping being application dependent.
Watchdog monitoring alarms	3 off inputs monitoring the external triplicated watchdog.

Table 5 System Alarms

3.5.9 Automatic Diagnostic Action

Certain actions, dependent on configuration, must be taken by the application logic on the result of certain error flags and combination of error flags.

3.5.10 Without Time Constraint Configuration

If a system is configured without time constraint (eg each critical process parameter is controlled by at least two separate digital output modules), then only annunciation of diagnostics is required.

3.5.11 With Time Constraint Configuration

If a system is configured with time constraint (eg any critical process parameter is controlled by a single TMR digital output module) then Global Output bit is used to start a timer equal to the time constraint of the Output Module and when this timer has elapsed an ESD command should be instigated. Example shown in Appendix 1

3.5.12 Long Process Time Constraint System

For systems controlling a process that has single inputs configured using the single slot hot repair facility then the "Single Slot Off-Line" error flag must be used to start a timer equal to the process time constraint. When this timer is elapsed an ESD command should be instigated.

3.5.13 Initialisation Flags

This flag indicates a wrong configuration of I/O modules or an I/O module or modules missing. Although these errors are inherently fail safe (eg when an on-line output module is removed its outputs automatically fail-safe).

It is recommended that this flag be used to instigate an orderly shutdown of the remaining part of the process.

3.5.14 MPP A, MPP B, MPP C

When an external TMR watchdog circuit is used to provide additional defence against common cause failure, these error flags are used to control the pulsing of the watchdog. The watchdog drive ladder network should be placed at the end of the networks.

3.5.15 Power Supply Failures

Each system chassis tolerates the loss of a single system power supply. The power fail alarm contacts on each system power supply should be available to be read by a digital input to allow the system power supply diagnostics to be reported.

When two external power feeds are supplied to the system cabinets the system power distribution must be designed to tolerate the loss of one of these feeds.

3.6 Application Software, Design, Verification and Validation

TriBuild provides a number of tools and facilities to aid safe application programming. A comprehensive 'help' facility is provided with TriBuild and this is supplemented by the Software Reference Manual 008-5206. There are also a small number of functions available with Triguard that must not be used for safety applications.

3.6.1 Non Safety Functions

The following function calls must **not** be used in Emergency Shutdown Safety Applications: -

- GOTO
- PAUS

Only the TUV approved library elements (marked with an *) should be used for safety functions.

3.6.2 Modularity and Version Control

The TriBuild Ladder Network Editor is a page by page editor allowing function and sub-function to be structured on a page by page basis. This facility should be used to provide structure to the application programme.

When modifying a ladder design version control must be maintained, and the systems designer must fully document changes.

3.6.3 Discretes and Register Validation

Using the facilities within the TriBuild Network Editor a Cross-reference list must be produced. This list must be used to ensure that no double usage of discretes or registers has occurred.

3.6.4 Power-Up Initialisation

The application logic must be designed that on power up all outputs are set to the 'off' safe state.

As part of the Triguard Release 3 program a new feature has been added to RTTS (8.30-008 and later versions) that permits a Triguard system to resume application logic execution automatically after power is restored to the main processors.

For main processor configuration details refer to revision 6 of the Triguard SC300E MPP Module User Manual. Switch settings allow the auto-restart function to be enabled, assuming battery-backed memory is being used to store both application logic and I/O status.

If this feature is employed then system designers must ensure that the system's I/O configuration and application logic are structured such that both operators and plant are not presented with a dangerous condition upon restoration of system power after a power outage.

3.6.5 Application Logic Verification

A peer to peer application logic code walk through should be completed prior to Test.

3.6.6 Application Logic Validation

Prior to the Acceptance Test the application logics should be fully functionally tested on the target system.

Particular care should be taken in the testing of the application logic if the system auto-restart feature is used.

3.6.7 Start-up Overrides

If the application requires certain safety permits to be overridden during the process start-up, the override logic must automatically time-out within the process safety time related to the start-up sequences.

Start-up overrides may only be enabled via keyswitch or password operator protection.

3.6.8 System Acceptance Test

The System Acceptance Test should at minimum cover mechanical inspection, electrical testing (isolation and earth bonding / continuity) and functional testing.

The System Acceptance Test harness should be configured to as closely as possible simulate the site functional conditions.

All Triguard SC300E input and output modules must have their 3-2-0 configuration checked and logged prior to the start of the Factory Acceptance Test (FAT).

In addition to a 100% Cause and Effect Validation (full Functional Test), the FAT should include as much random testing as is practical as well as test to confirm both fault tolerance and maintainability.

Particular care should be taken in the testing of the application logic if the system auto-restart feature is used.

3.6.9 Application Software Documentation

The TriBuild Software Development Tools provide version control, and it is mandatory that the application software developer documents the networks thoroughly and provides tractability of changes by adding the appropriate change description.

Typical well-documented networks are given in Appendix 1.

3.6.10 Application Logic Driven External Triplicated Watchdog Timer

The application logic used to drive the external triplicated watchdog timer is used to confirm that the application logic is operating correctly and the outputs are being written to. The triplicated watchdog timer should never be required to operate; however, it is an effective measure against unknown systematic faults, which cannot otherwise be detected.

The outputs from the external watchdog can be used to shutdown the field power supplies or disconnect the field power to the final elements on the systematic failure of 2 or more processors. The configuration of the output of the external watchdog will depend on the end users application. The external watchdog timer will be configured for 2oo3 operation and must be tested periodically as recommended in the user manual.

3.6.11 Use of Triplicated Watchdog Timer with Remote Chassis.

When used in a system with one or more remote chassis, the voted output of the external watchdog timer is used to remove both power feeds to the chassis power supplies (PAC or PDC24) of the main chassis. This will ensure that all output modules will fail to a known safe state 2.64 seconds after the external watchdog trips by the common interface watchdogs.

The fall back state is defined by the links on the digital output modules, for ESD system this is GTZ (Go To Zero).

3.7 TriBuild, Network Examples

Refer to Appendix 1 for example networks detailing the Mandatory Application logic required.

3.8 Environmental Functionality

To meet CE Emission requirements the Triguard SC300E System must be mounted within a standard Rittal type cabinet with EMC seals fitted on all doors.

3.9 Security

All system cabinets must be fitted with keylocks to enable the proper control of access to the Triguard SC300E Safety System.

Software security access via the password protection scheme of TriBuild will be the responsibility of the end user. The System Integrator must ensure that the end user is fully aware of the facilities of the TriBuild password protection scheme.

Each processor, when in normal operation, should have its front key in the run position and the keys removed to further prevent unauthorised access. It is the responsibility of the end user to ensure proper maintenance control of the Triguard SC300E Safety System.

3.10 System Power Supplies

Each system and I/O chassis requires two power supply feeds. These feeds must be separately protected and ideally should be derived from two separate secure sources.

3.11 Field Sensors and Final Elements

It is the responsibility of the System Integrator to review the proposed field equipment to ensure the correct quality of Sensors and Final Elements is being used for safety loops.

3.11.1 Field Power Supplies

All field power supply failures must in principle be fail safe. The field power supply configuration will be at a minimum 100% functionally redundant (any single power module failure leaves the bulk power supply in the position of being able to maintain 100% load).

3.11.2 Field Power Distribution

Distribution of the field power supply to the field will be through power supply breakers or fuses, any failure must be annunciated. The Power Distribution and Alarm Panel PDD24 is a suitable product for this application.

The Triguard SC300E termination cards provide individual loop fusing with alarms.

3.11.3 Field Power Diagnostics

Each redundant power module will provide diagnostics fault detection. All faults in external power supply modules connected directly to the system (eg field power supplies) must be alarmed and reported.

4 Installation And Commissioning

4.1 Introduction

The installation and commissioning phase of a Triguard SC300E Project must be carefully planned and will include the final system validation prior to the plant going on-line.

The Triguard SC300E TMR User Manual 008-5197 must be referred to. The System Integrator shall also have provided a tailored manual (incorporating the above standard manual) for the specified site.

The Installation phase should include at minimum mechanical inspection, electrical testing (isolation and earth bonding / continuity) and functional testing.

The installation and commissioning phase also provides the last opportunity to carry out and validate application modifications prior to the plant going live.

4.2 Site Planning and Environment

Confirmation must be obtained that the location and environment, both in normal and fault conditions (eg air conditioning failing), fall within the bounds of the Triguard SC300E environmental specification.

Maintenance access to the system cabinet must be confirmed and access to the safety system must be by authorised key holders only.

4.3 Process Field Connection

All input and output safety and safety related loops must be tested, including all field devices (the sensors and final elements) and the results recorded during the loop test period.

4.4 Systems Start-up and Shutdown Procedures

The System start-up and shutdown procedures are documented in detail in the Installation and Commissioning Manual 008-5204 and these must be adhered to at all times.

This manual should always be provided as part of the bespoke Installation and Commissioning Manual provided by the System Integrator for all Systems.

All switch positions must be confirmed as correct with respect to the User Manual documentation.

4.4.1 General Description - Start-up Procedure

Before power is provided the main processors must have their keyswitches in the reset position.

Field and system power is provided to the system. A momentary switch to enable this function should manually reset the watchdog. At this stage the processors are brought on-line and the system started.

The process start-up sequence will be Process dependent and documented in the Bespoke Operation Manual.

The Version of RTTS should be confirmed by commanding the System History Report. This report provides a print of the version number of RTTS in its header. The Library version is linked to TriBuild and the version number can be confirmed during the start-up window.

4.4.2 General Description - Shutdown Procedure

The process shutdown sequence will be Process dependent and documented in the Bespoke Operation Manual.

If power is to be removed from the Safety System, this should only be instigated after a safe process shutdown and the instigation of appropriate manual safety interlocks. The process and plant must be brought to a safe state and all hazardous materials removed.

System power should first be removed from the main chassis and subsequently the external chassis power should then be removed from the field outputs and inputs. The processor should then be set in the reset mode by front panel keyswitch operation.

4.4.3 Application Changes During Commissioning

In the ideal situation there should be no application changes during the commissioning phase of a Safety Systems Project. When, however, changes are required it is mandatory to follow the full life cycle change sequence, including re-confirmation of HAZOPS and full validation. All changes must be fully documented and under version control to the same standard as the original system design. All changes must be completed prior to the final Site Acceptance Test Validation.

4.4.4 Site Acceptance Test Validation

Prior to the plant going 'live', a full system validation (proof test) must be completed. This validation follows the cause and effect/fault schedule using the plant sensors and final elements as well as the logic solver.

Where practical, random causes should also be tested during this final validation cycle.

Fault tolerances and maintainability should also be re-validated during the Site Acceptance Test (SAT) including, where practical, field sensors and actuators.

4.4.5 Permits to Work

Prior to the plant going "live" the formalised permit to work procedure for the plant must be in operation.

4.4.6 Module Slot Security

Prior to the plant going "live" a slot polarisation-coding blocks on each SC300E chassis should be sealed to prevent polarisation changes during maintenance operation.

5 Operations

5.1 Introduction

The Operations Section of this manual covers only the aspects related to safety of operating a Triguard SC300E Safety Programmable Logic Controller configured for an Emergency Shutdown Application.

The Operations and Maintenance Manual provided by the System Integrators will cover all application aspects with respect to the operation of the system and all standard maintenance procedures. All operators must be fully conversant with this manual. The supplied Operations and Maintenance Manual will include the standard Operations and Maintenance Manual 008-5202.

5.2 Training

All operators of Triguard SC300E Safety Systems must have completed the Triguard SC300E Operators Training Course. It is recommended that operators be re-trained on a SC300E refresher course every 24 months.

5.3 System Start-up

Operators must ensure that there is no dangerous material within the plant or process prior to the start-up of the Triguard SC300E Safety System

An auditable permit to works system must be in operation before any system/process start-up operation occurs.

Trained maintenance staff will only complete the system power-up. The Operational Start-up procedures documented in the Operations and Maintenance Manual must be followed in the order presented.

5.3.1 Process Loading and Start-up

Before the process is re-loaded into the plant and the process plant started, the Safety System must be confirmed to be in full operation and 100% healthy. If during the system start-up procedure errors still remain in the system, maintenance must ensure that these errors are corrected before process load and start sequence commences.

5.4 System Operation

The detailed operation aspects of the supplied Safety Systems will be covered in the bespoke Operations and Maintenance Manual supplied by the System Integrator.

The following procedures, however, must be followed to ensure the continued and safe operation of the system and plant.

5.4.1 Maintenance Alarm

All maintenance alarms must be immediately brought to the attention of maintenance by operations to enable repairs to be carried out within the specified Mean Time to Repair.

5.4.2 Maintenance Actions

Any maintenance actions specified to be carried out by Operations (eg lamp test) must be carried out as specified and results logged.

5.4.3 Process Trips and Events

If during the course of normal operation a process trip or event that causes action by the safety systems should occur, then all results must be logged and confirmation that the correct safety action demanded occurred should be made.

Before restarting the process after an event, the plant safety supervisor must confirm that the plant is safe to be re-started.

5.4.4 Maintenance Engineering Station

The TriBuild Maintenance Engineering Station should not be connected to the system during normal operation.

5.5 System Shutdown

The Safety System would normally only be shutdown during a planned major plant maintenance cycle. During this period it is likely that both major equipment will be dismantled and serviced, and possible process and system parameters modified.

If process and system parameters are to be modified, then Section 7, Maintenance and Modification must be adhered to.

5.5.1 Process Shutdown

Before the Triguard SC300E Safety System is shutdown the process must first be safely shut down and the plant brought to a safe/neutral state.

This would normally require that all hazardous materials are removed and the process purged.

5.5.2 Triguard SC300E System Shutdown

The Triguard SC300E System Shutdown will be documented in the supplied bespoke Operations and Maintenance Manual specific to the plant.

In principle, the following sequence of power down is followed: -

- 1) Remove power to main chassis.
- 2) Remove power to slave chassis.
- 3) Remove power to all fail-safe outputs, final elements and field sensors.
- 4) Turn off main panel power breakers.

6 Maintenance And Modifications

6.1 Introduction

This section of the Safety Manual covers the safety aspects of two life cycle functions of a Triguard SC300E System, Maintenance and Modifications. The Operations and Maintenance Manual supplied by the Systems Integrator will cover all standard operational and maintenance procedures and be written specifically for the systems configuration supplied.

With a fault tolerant system such as the Triguard SC300E one of the primary tasks of maintenance is to maintain the system in a 100% healthy state to enable the full power of the fault tolerance provided, to be delivered to the safeguarding of the plant. Although the Triguard SC300E is inherently fail-safe, on a second major fault it should be noted that an operating plant is inherently more safe when operating than during a start-up or shutdown phase. Therefore, unnecessary trips due to poor maintenance should be avoided.

6.2 Routine Maintenance

As with all safety-related systems, there will be a number of routine maintenance tasks required for any Triguard SC300E supplied. The routine maintenance tasks are documented in the Operations and Maintenance Manual supplied with the System by the System Integrator and the relevant Product User Manuals. This section deals only with specific safety aspects related to routine maintenance.

6.2.1 System Verification

When first connecting the TriBuild workstation to the Triguard System the on-line system is checked against the off-line system stored on the workstation. If the systems are different a warning is given and the off-line system must be closed down and the correct system selected prior to connecting to the Triguard system.

6.2.1.1 Application Logic Verification

The application logic can be verified by using the TriBuild Ladder compare facility. This compares the on-line ladder logic with the off-line ladder logic held on the TriBuild workstation.

6.2.2 Diagnostic Alarms and Messages

The structure of the diagnostics in a Triguard SC300E System is both hierarchical and fail-safe. In principle, whenever the first hardware fault is found the fault call indicates this error by changing the status of the relevant fault call bit.

Certain fault call bits are specific and down effectively to module level (eg CPU health). The majority of the input and output faults, however, appear as monitor errors, LFD errors, data/vote errors or initialisation errors.

As stated in the application section, the initialisation error will cause, by correct use of application logic, a shutdown to occur as this may indicate the removal of a vital input or output module. These initial diagnostic alarms are readily reported to the operator, by LED's, lamps, alarm sounders, printer messages or alarm messages on the operator display console and should initiate action by Operations to inform Maintenance that a problem exists.

With the exception of catastrophic failures, which in general would need to be personnel instigated (eg incorrectly removing an on-line module) all first failures are tolerated without the need to shut down the process.

6.2.2.1 Detailed Diagnostics

Having received a diagnostic alarm the maintainer, having been given a permit to work, would gain access to the system cabinets via keylocks.

The first level of detailed diagnostics is visual as each module in the Triguard SC300E System has a green health led and the faulty module should already be indicating its fault by extinguishing the health led.

In the unlikely event that all health LED's are still on, the next level of diagnostics evaluation requires the use of TriBuild. The TriBuild Administrator will have given all maintainers maintenance writes of access that will allow them to view diagnostics and, where appropriate, networks but would not allow on-line changes. This access control is by password protection (and, of course, cabinet keylock) details of which are provided in the TriBuild User Help facilities.

6.2.3 Module Change-Out

All Triguard SC300E Modules can be changed on-line without disturbing the safeguarding of the process.

It is recommended that all spares be available from a spares test system, where the health of the spare module can be confirmed prior to change-out.

Off-line modules must be tested periodically.

6.2.3.1 Input and Output Modules

The spare module should first be visual checked, in the case of input and output modules this should include the fact that the coding blocks are correctly fitted (eg operation mode, GTZ...) and that the settings of the fallback links are correct eg operation mode 3-2-0 (GTZ and HW for output modules).

In the case dual slot configuration of Triguard SC300E input and output modules, the new module should be inserted into the relevant hot repair slot and after the module has confirmed its health by powering the health led, the maintenance switch may be toggled which will request the hot repair cycle to be initiated.

The hot repair cycle is initiated by the main processors and is indicated by the flashing of the LED's on the new module. It culminates with the on-line LED's of the new module going "on" whilst at the same time the on-line LED's of the module to be removed goes off.

When this cycle has been successfully completed, the location screws on the new module should be tightened and the faulty module removed for repair.

The error clear should now be operated to bring the system back to 100% operation by clearing the error history, which will allow any new faults that occur to be readily diagnosed.

6.2.3.2 Main Processor Modules

The spare processor module should first be visually checked to confirm the configuration switches are correctly set.

If a warm-start keyswitch has not been made available by the application configuration, the TriBuild Workstation should be connected to the console port and brought on-line.

Turning the processor keyswitch to the reset position should then halt the faulty processor and then the faulty processor should be removed.

The new processor should now be plugged in to the vacant processor slot with the keyswitch set in the reset position. The keyswitch is then turned to the 'run' position. The processor will then run through its off-line diagnostics to re-check its health, which is indicated by the front lights sequencing and the green health light being turned on.

When this has completed, the front LED's are extinguished for approximately 3 seconds and then are illuminated, the processor is now ready to be warm started into the system.

The warm start command instructs the two operating processors to allow the warm starting processor to read their memory. The warm starting processor first reads the system data and programme code which is static and finally, when this is completed, it requests the two operating processors to halt for approximately 0.5 seconds whilst it reads the varying data. This being completed all three processors resume full operation.

In the event that an error is found in the warm starting processor during this sequence and it fails to warm start, the two operating processors continue on without the third processor.

On the successful culmination of the system repair the error clear should now be operated to clear the error history to enable new faults to be readily interpreted.

6.2.3.3 Bus Buffer Module

The spare bus buffer module should be visually checked against the user documentation. The faulty bus buffer module can now be removed and replaced by the spare module. The error history clear should now be operated to allow any new faults that occur to be readily diagnosed.

6.2.3.4 Power Supply Module

The spare power supply module should be visually checked.

The faulty power supply should first be switched off using the front panel switch before unscrewing the chassis fixing screws and then removed.

The spare module should then be plugged in and powered up. The error history clear should now be operated to allow any new faults that occur to be readily diagnosed.

6.2.3.5 History Clear

During a maintenance repair activity the history error report should first be printed before the fault bits are cleared by use of the error clear facilities within TriBuild. This action is important as by clearing the errors all historical errors are lost and any new errors that occur will be readily diagnosed. Also clearing the error bits will ensure that if a time constraint timer is configured in the application, this will be reset, after one complete LFD test cycle, until the next error appears.

6.2.4 Sequence of Repair

Certain faults, for example Power Supply, Main Processor and Bus Interface Module, will give rise to both alarms associated with the fault as well as additional alarms. For example when one of the dual power supply modules in a chassis fails additional to the power supply failure alarm, each I/O module within the chassis will be reporting that one of its power supplies has failed and indicate a health problem. It is therefore important to repair the SC300E in a logical order or sequence.

The following order should be followed assuming fault indication for each item is given: -

Priority

1	Chassis Power Supply Units	
2	Main Processor Units	MPP
3	Bus Interface Units	MBB
4	I/O Modules	
5	Field Connection	

After each repair the history should be cleared and the next item to appear dealt with.

6.2.5 System Time Constraints

When the configuration of the Triguard SC300E includes the requirement of a system time constraint the process must be shut down if a repair has not been successfully completed after the system time constraint has elapsed.

6.2.6 Life Cycle Proof Test

The safety integrity level requirements and field device configuration will determine a Life Cycle Proof Test for each safety loop.

The Life Cycle Proof Test ensures that all devices in the safety loop, from sensor to final element, operate correctly.

The application of a certified Triguard SC300E System as the logic solver does not remove the requirements for full safety loop proof testing.

6.2.6.1 Watchdog Maintenance

The external watchdog should be checked during the normal proof test maintenance cycle. The watchdog configuration links must also be inspected during commissioning and maintenance.

6.2.7 Maintenance Overrides

The user must maintain strict control of maintenance overrides. It is recommended that the user follows TUV maintenance override procedure version 2.2 0.8 September 1994.

When the TriBuild Maintenance Override facility is used to apply maintenance overrides directly, the number of maintenance overrides in place at any one time will be limited to the maximum number configured by the system administrator. Overrides applied by the use of the TriBuild workstation will have limited time duration related to the shift operating time (typically 8 hours). A warning is provided by the system that the maintenance overrides will be automatically removed unless reinstated.

5.3 Modifications

Wherever possible on-line modifications to a safety system should be avoided. If on-line modifications are required, the complete safety case must be documented and approved by the plant safety committee.

If the proposed modifications are not extensive, then providing the precautions documented in the lifecycle models of IEC61508 and IEC61511 (Draft) are followed and providing the following additional verification measures are taken, it will not be necessary to validate the complete safety system.

WARNING

If in the process of a modification of a ladder network an energised coil (output) is deleted and the coil(s) are not used elsewhere on other networks, then the Output State will be maintained in the last valid state (energised).

6.2.8 Minor Modifications

The following verification measures should be followed on all minor modifications to avoid the necessity to complete a full system validation.

Verification should be completed and documented that the configuration changes required and only those required has been implemented. These are recorded in the Build report log in the Build directory

Verification should be completed and documented that the logic changes required and only those changes required has been implemented. Before and after ladder listings and compare facilities should be used.

Verification using the register and discreet cross-reference that no double use of registers or discrettes has occurred should be completed and documented.

Providing the results from the above verification are positive, then only the implemented changes need to be tested before they are finally brought on-line.

For all extensive changes the following procedures must always be followed.

6.2.9 HAZOPS

The required modification must be subjected to a full Hazard Analysis (Hazard and Operability Study) including all possible effects on the unchanged parts of the system.

6.2.10 Design

The modification design must follow the same full life cycle process as the original design described in Section 4.

6.2.11 Verification and Validation

Full off-line verification and validation, as described in Section 4 both for Hardware and Application Software, must be completed prior to installation.

6.2.12 Installation and Commissioning

All safety aspects given in Section 5 of this manual must be adopted during the installation and commissioning phase of a modification.

6.2.13 Acceptance Test Validation

A system validation (cause and effect test) will be implemented for the modified parts of the systems prior to bringing the modified parts of the system on-line.

6.2.14 Personnel

Only personnel with the correct level of training and expertise, both in safety and process knowledge, will be authorised to implement system modifications.

6.3 Training

All maintenance staff that are required to work on the Safety System will complete a one week maintenance training course and will attend refresher courses every 24 months.

All maintenance staff that are required to perform modifications to an installed Triguard SC300E Safety System will attend an additional one week course on Triguard SC300E System Engineering prior to the implementation of the system modifications.

6.4 Security

All system cabinets are fitted with keylocks to enable "permit to work" controlled access to the SC300E Safety System.

The TriBuild maintenance workstation is provided with multi-level password protection to ensure only qualified maintenance staff has access to the Triguard SC300E Safety System.

Each processor, when in normal operation, should have its front key in the run position and the keys removed to further prevent unauthorised access. It is the responsibility of the end user to ensure proper maintenance control of the Triguard SC300E Safety System.

6.5 Failure Reporting

All hardware or software failures or faults that occur during the operational life of the Triguard SC300E Safety System must be logged and analysed for their safety impact.

All failures or faults must be reported back to the system supplier.

It is the responsibility of the end user to ensure that an accurate reliability database is maintained for all equipment used for safety related functions.

6.6 Maintenance Completion

When a modification or maintenance cycle has been complete and the system is restored to operating health, the TriBuild Maintenance Station should be disconnected from the running SC300E System.

7 De-Commissioning

7.1 Introduction

All process plants eventually arrive at the end of their useful operational economic life. Hazardous plants that normally would have a Triguard SC300E Safety Controller in operation safeguarding the plant must be de-commissioned in a safe and environmentally friendly manner.

Before de-commissioning or disposal activity can occur, an impact analysis shall be carried out to assess the impact on the functional safety of the Triguard SC300E System and any adjacent plant or processes that may still be in operation. The de-commissioning plan must fully take into account the results of this analysis.

7.2 Final Process Shutdown

The operation and maintenance of the plant must be fully and professionally manned and managed through the de-commissioning period.

The final process shutdown initially would emulate all previous major maintenance shutdowns in the sequence of shutdown operation.

Once the plant is in its final safe state, all inflammable and hazardous material must be removed from the plant safely and environmentally correctly disposed of or recycled into other operating plants.

A full clean purge sequence must then be operated and the plant must be certified as fully safe by the appropriate authority before power is finally removed from the safety system.

7.3 Dismantling and Removal

Before the dismantling and removal operation can occur the Triguard SC300E System and its related field equipment must be fully electrically isolated.

7.3.1 Electronic and Electrical Modules

All electronic and electrical modules should be removed from the system and the parts removed from the site by electrical and electronic disposals/recycling specialists.

7.3.2 Mechanical Items

The majority of mechanical items will be manufactured of steel and aluminium. These items should be separated and disposed of through the appropriate recycling agency.

7.3.3 Safety Precautions

On no account should any Triguard SC300E Products or wiring be locally incinerated.

8 Appendix 1 - Safety Networks

The following networks provide examples of safety network configurations.

Network 1

Input and Output Call
Fault Call
Single Slot Hot Repair Time-out Shutdown
PIM INIT Fault Shutdown
2oo3 Watchdog Vote Shutdown

Network 2

System Repair Time Constraint Shutdown

Network 3 & 4

Diagnostic Alarm Annunciation

Network 5

USR3 Analogue Test
1Hz Clock (example)

Network 6 & 7

Fail Safe Analogue Alarm Processing (example)

Network 8 & 9

Typical Logic's

Network 10

TMR Watchdog Drive

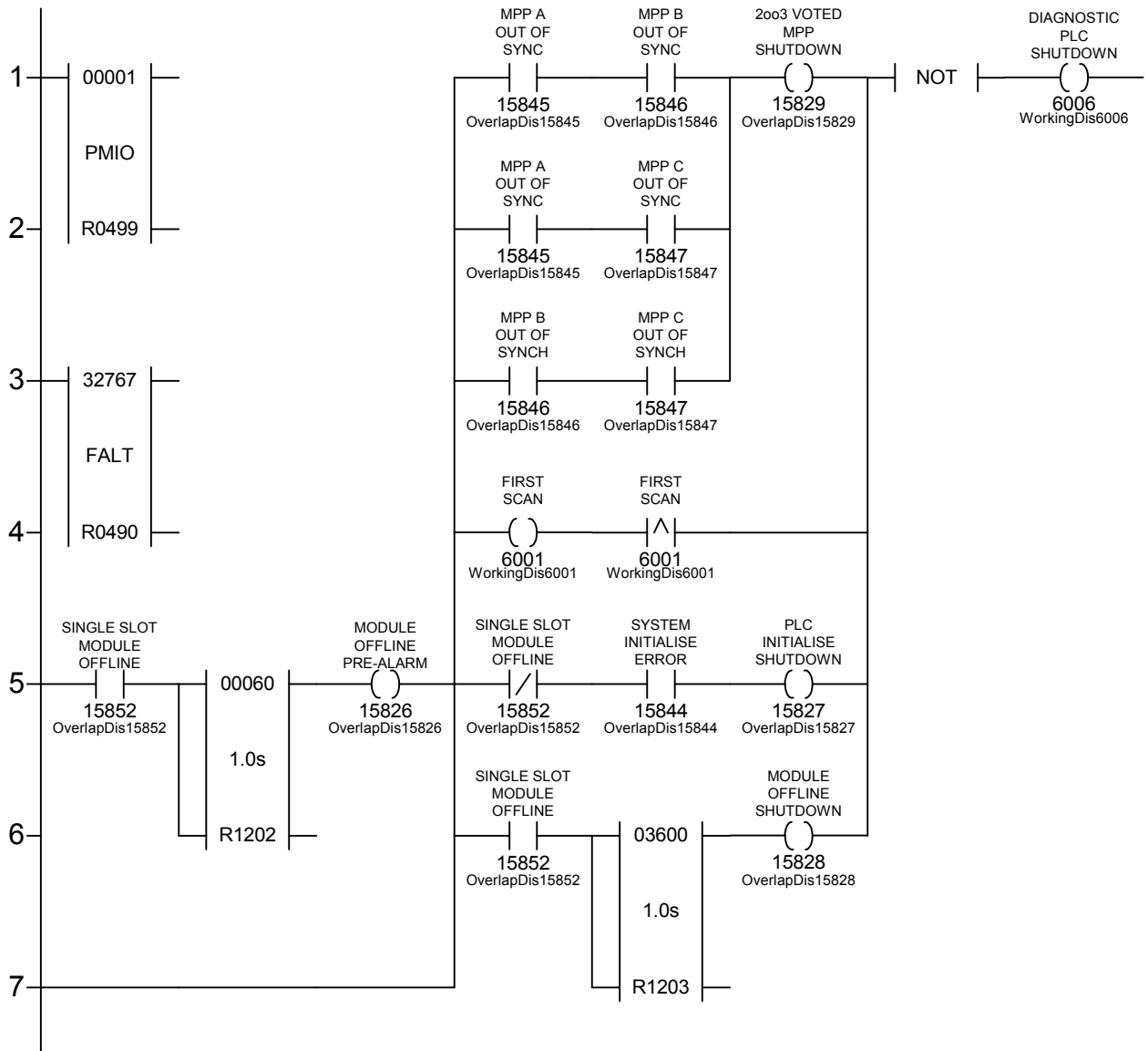
Network 11

Communication of diagnostics to DCS using the GDIA call

Network 12

Configuration of Analogue Outputs

Network 001 - Input Read / Output Write / Mandatory System Diagnostics
 Scan Rate 00030 ms
 Label 01002 Enabled

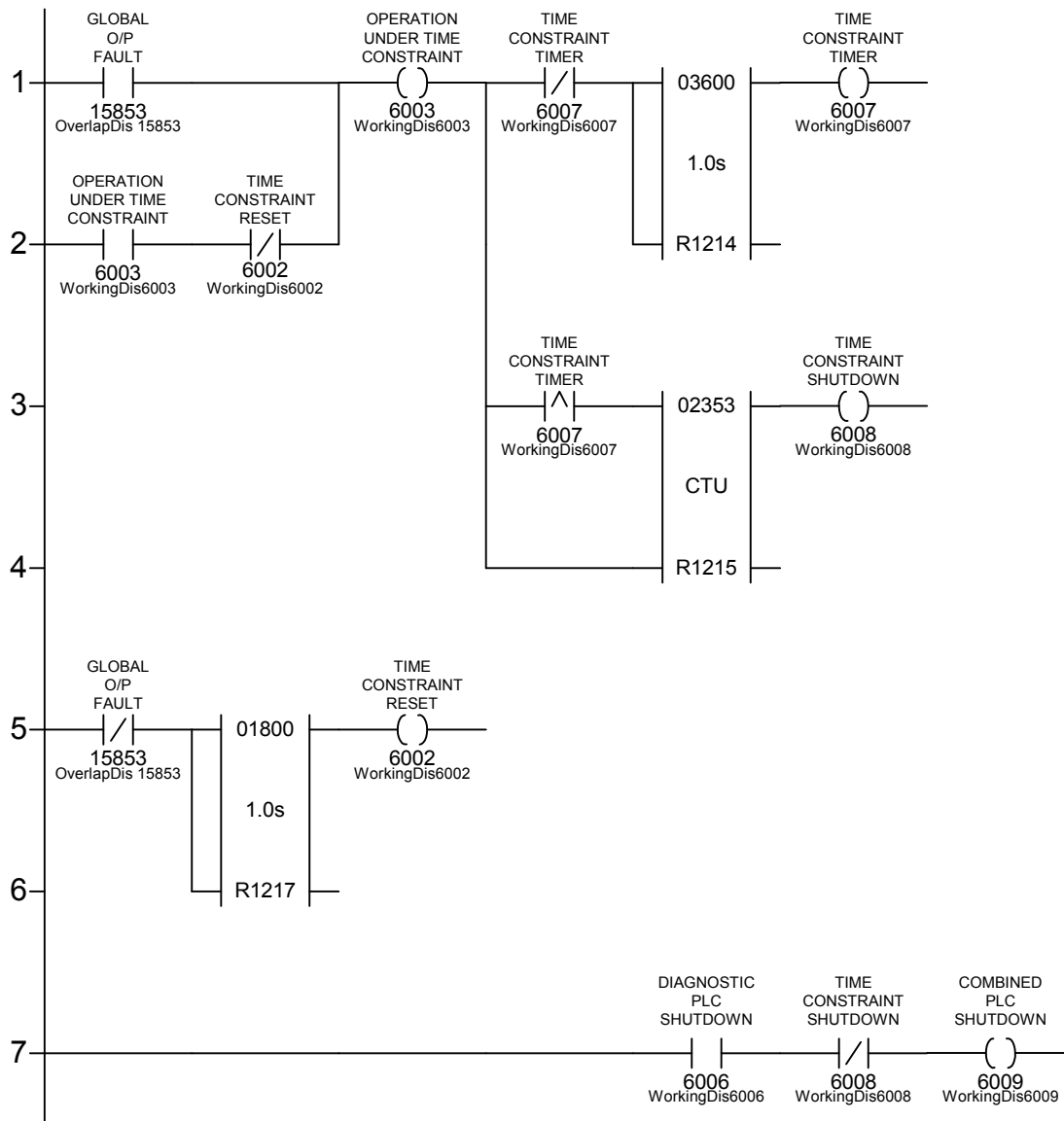


Mandatory Network (except Register No/Discrete No/Timer values).

PMIO call 1 is used to read/write all I/O points in Table of operations 1. The FALT call transfers all system diagnostics to register 490. 32767 is a mask of 15 bits that can be used to configure the call output. Note this mask does not inhibit any diagnostics. Discrete 15826 is a pre-alarm generated 60 seconds after any I/O module (including serial I/O modules) is taken Off-line. After returning an I/O module On-line the system diagnostics history must be cleared to reset this alarm.

The ESD logic is tripped (via Discrete 6006) if only one processor is running, on start up, or an critical I/O module is Off-line for more that the time set in timer R1203, or an I/O module is removed from the chassis without first being taken Off-line, or a I/O chassis is lost to be system by total power failure or loss of two MBB modules.

Network 002 - System Repair Time Constraint and Diagnostic Shutdown.
 Scan Rate 00030 ms Label 01004 Enabled

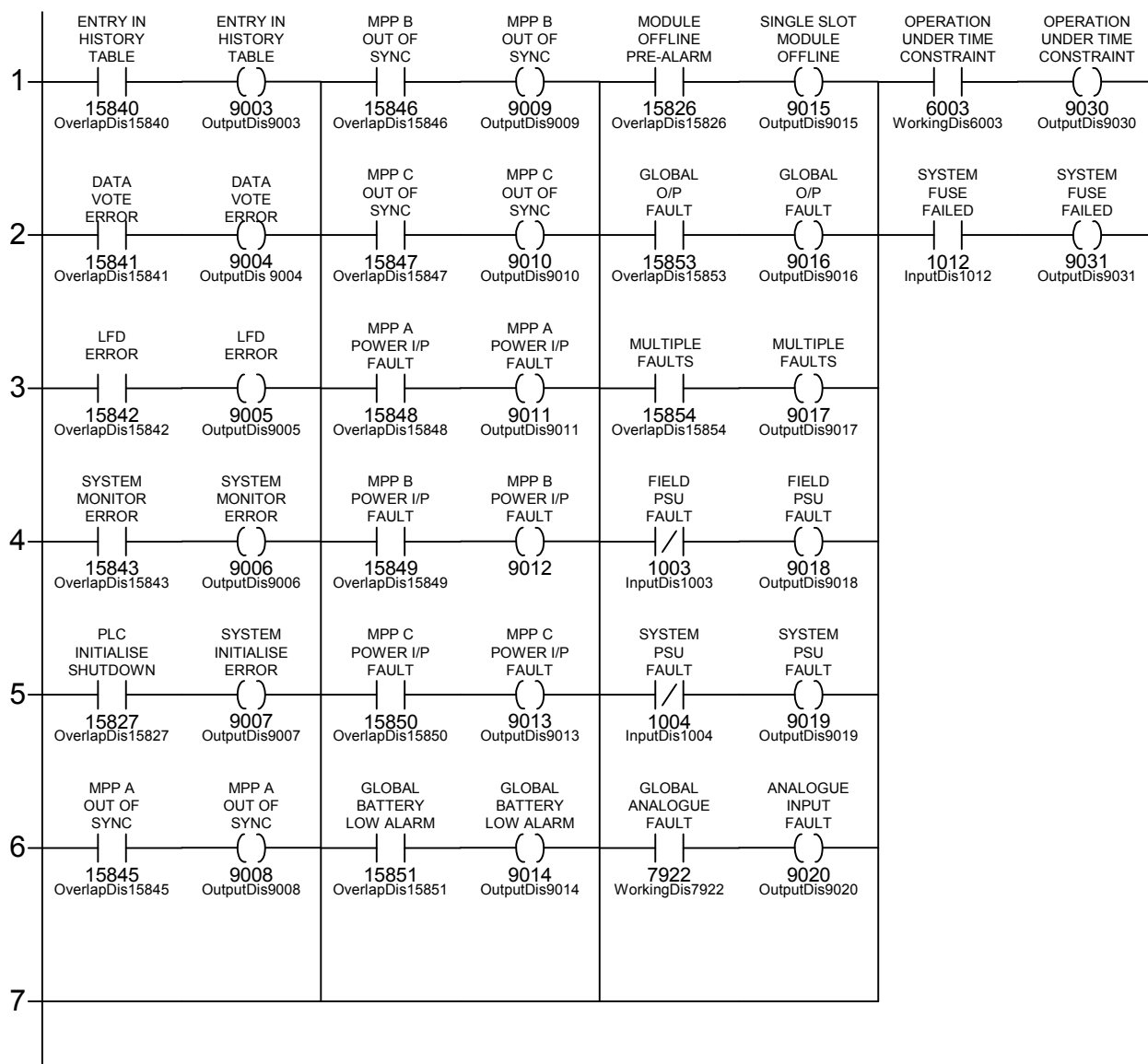


If the system has any single element safety outputs, or any dual element safety outputs are configured on a single output module than the system must be configured with a time constraint (Mandatory). This time constraint is set in hours in the Up counter (Minimum 2353 hours for SIL 3, 7440 hours for SIL 2 or 23528 hours for SIL 1). The Time Constraint counter and timer is reset once the Output Fault is cleared and remains clear for the system test time (set in the system test time timer R1217). The system test time is calculated as equal to the Number of Modules x 20 seconds).

The Time Constraint shutdown (discrete 6008) is combined with the Diagnostic shutdown (discrete 6006) to give a single PLC shutdown (via discrete 6009). This should be latched within the Application logic.

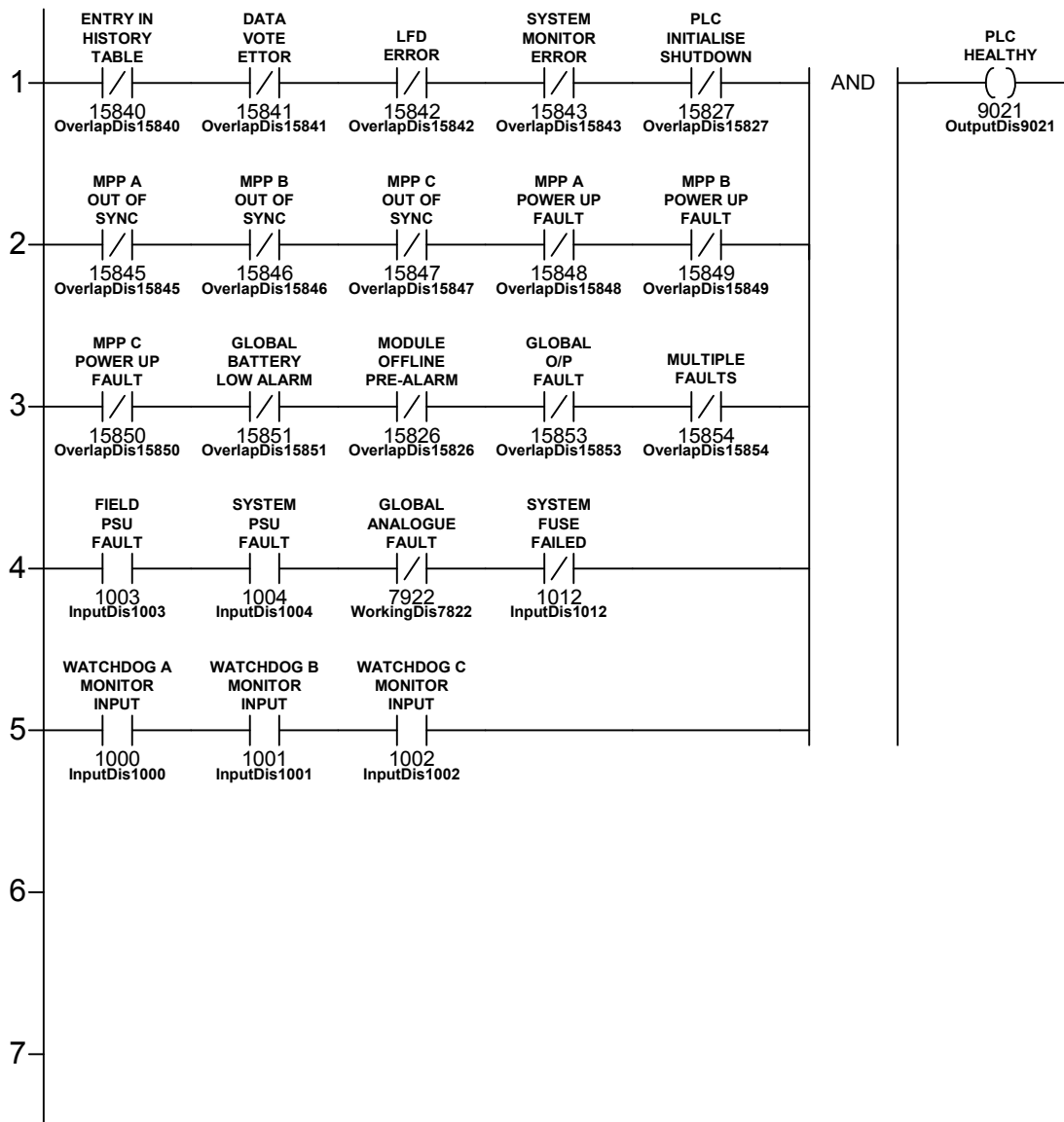
Network 003 - Individual PLC Diagnostic Annunciation.
Scan Rate 00030 ms

Label 01005 Enabled

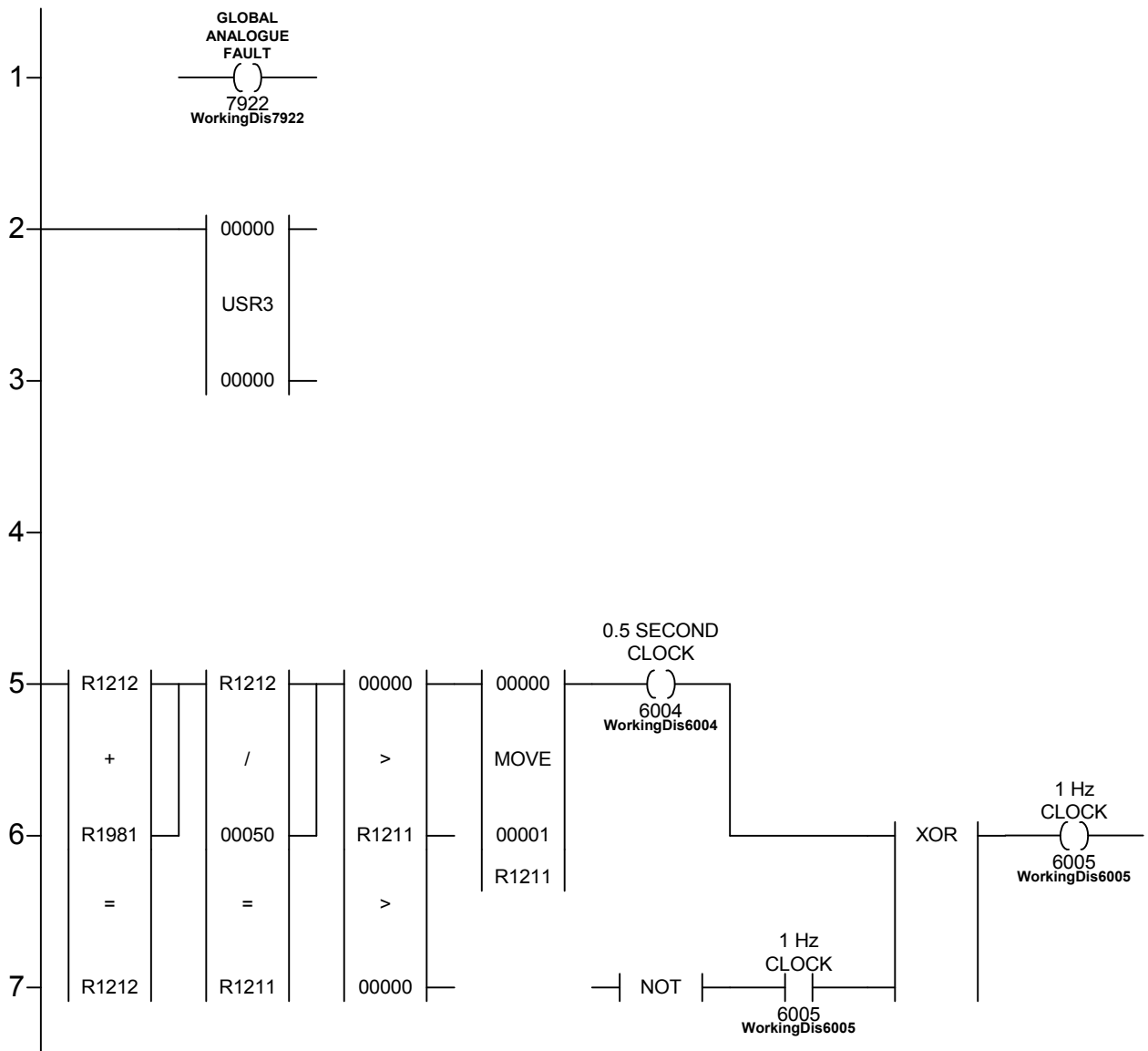


The diagnostic alarms from the FALT call element and diagnostic logic in the previous networks are individually annunciated.

It is mandatory that these alarms are annunciated but the method by which is done is user configurable. eg. Via hardwire annunciator outputs or via serial communications outputs.



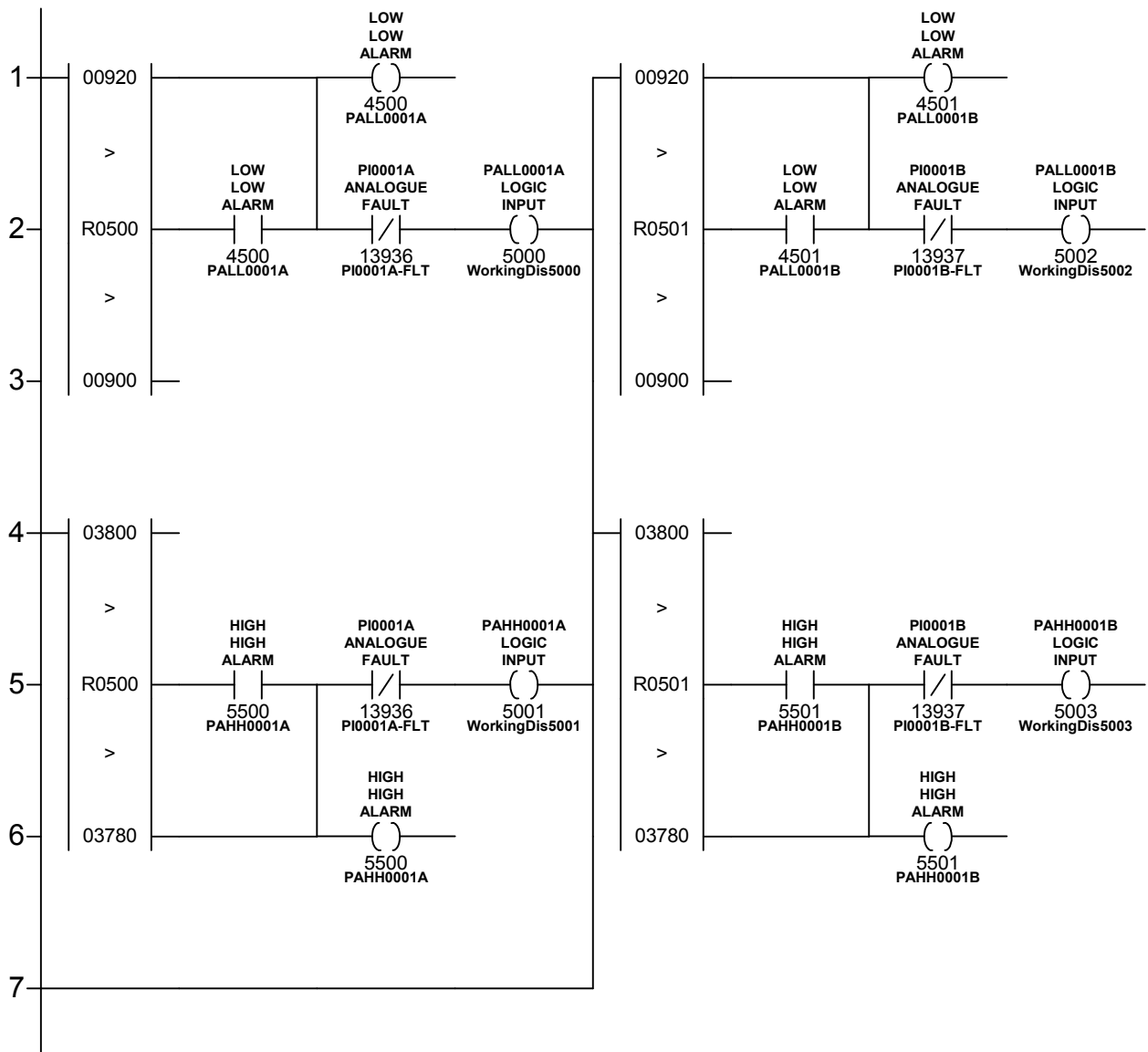
Discrete 9021 is common alarm to provide a single alarm annunciation of a PLC fault (Mandatory).



USR3 contains the Analogue Test and Event Processing Functions, Not Mandatory.
 Discrete 7922 is set to logic zero to reset the analogue test logic in USR3, if used.

Not Mandatory - Discrete 6004 is a one scan clock that is true every 0.5 seconds with no accumulative error, unless the scan time is set to greater than 0.5 seconds.
 Discrete 6005 is a 1Hz clock with equal mark/space ratio. It can be used to flash lamps.

In these example networks the 1 Hz clock is used to pulse the Watchdog outputs. The Watchdog outputs must be pulsed at minimum every 5 seconds and the logic for pulsing these outputs must be in the last ladder network. This is Mandatory.



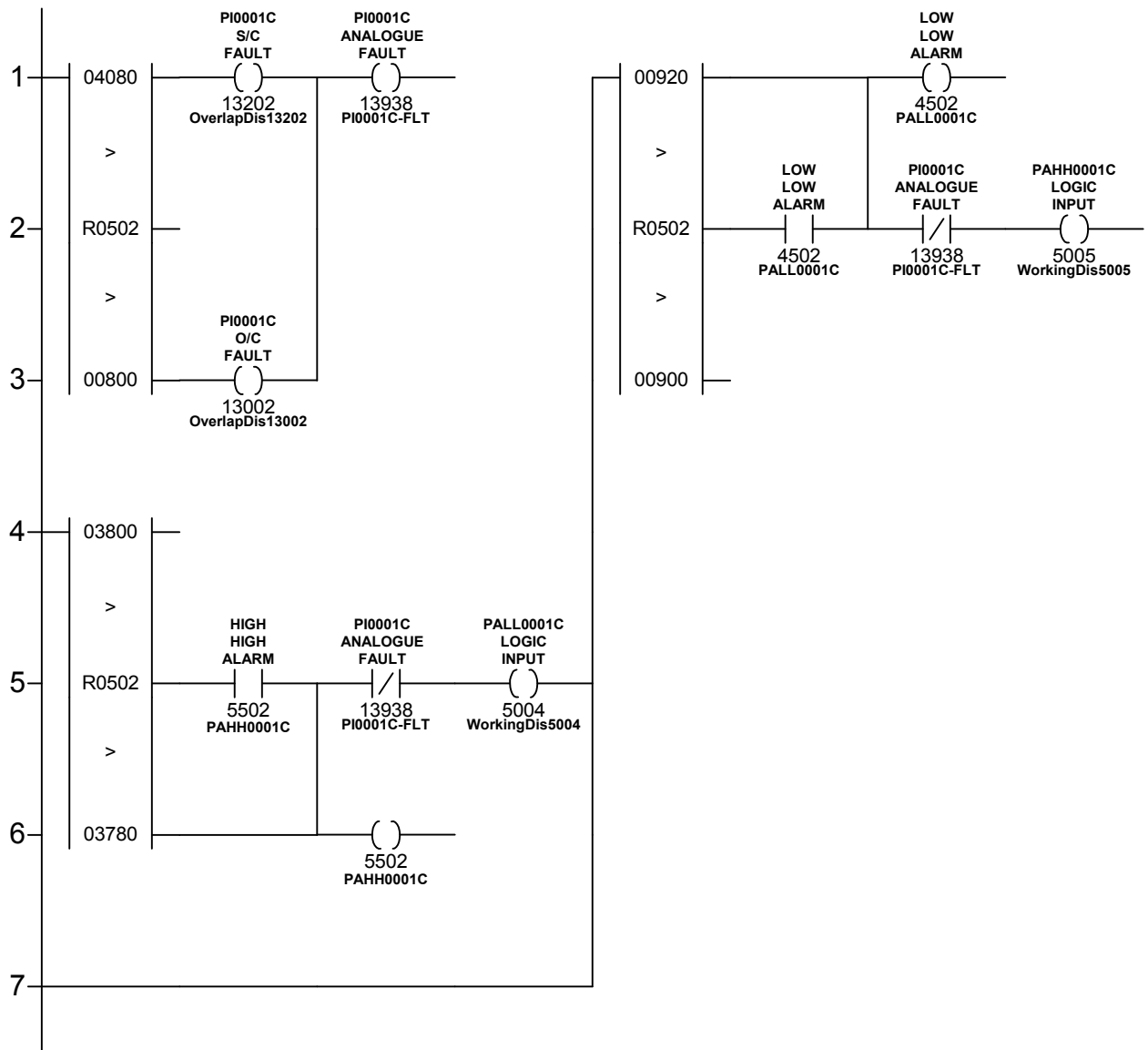
If safety critical analogue inputs are used, the alarm logic generated must include fail safe logic. This is Mandatory. A number of methods are available to generate fail safe digital logic inputs from analogue inputs, an example utilising the USR3 Analogue test package is given above (The values used are those given in the default Analogue test configuration).

The example above is for a single channel with both high 3800 and low 900 alarms.

The above circuit includes user configurable hysteresis on the alarm values (set in example to 20 bits) and allows for up to 4 analogue alarm levels to be processed on a single network. Alarm status are configured to be identical to digital alarm status i.e. Logic 1 Normal, Logic 0 Alarm.

Alarm annunciation is independent of the fail safe logic input and the O/C & S/C alarms are generated by the USR3 package with the common fault bit used to give a fail safe logic input.

If 2 faults are diagnosed on an analogue input channel the module is marked as bad and analogue input is given a negative value 8000H. This condition gives an O/C fault and trip the fail safe logic.

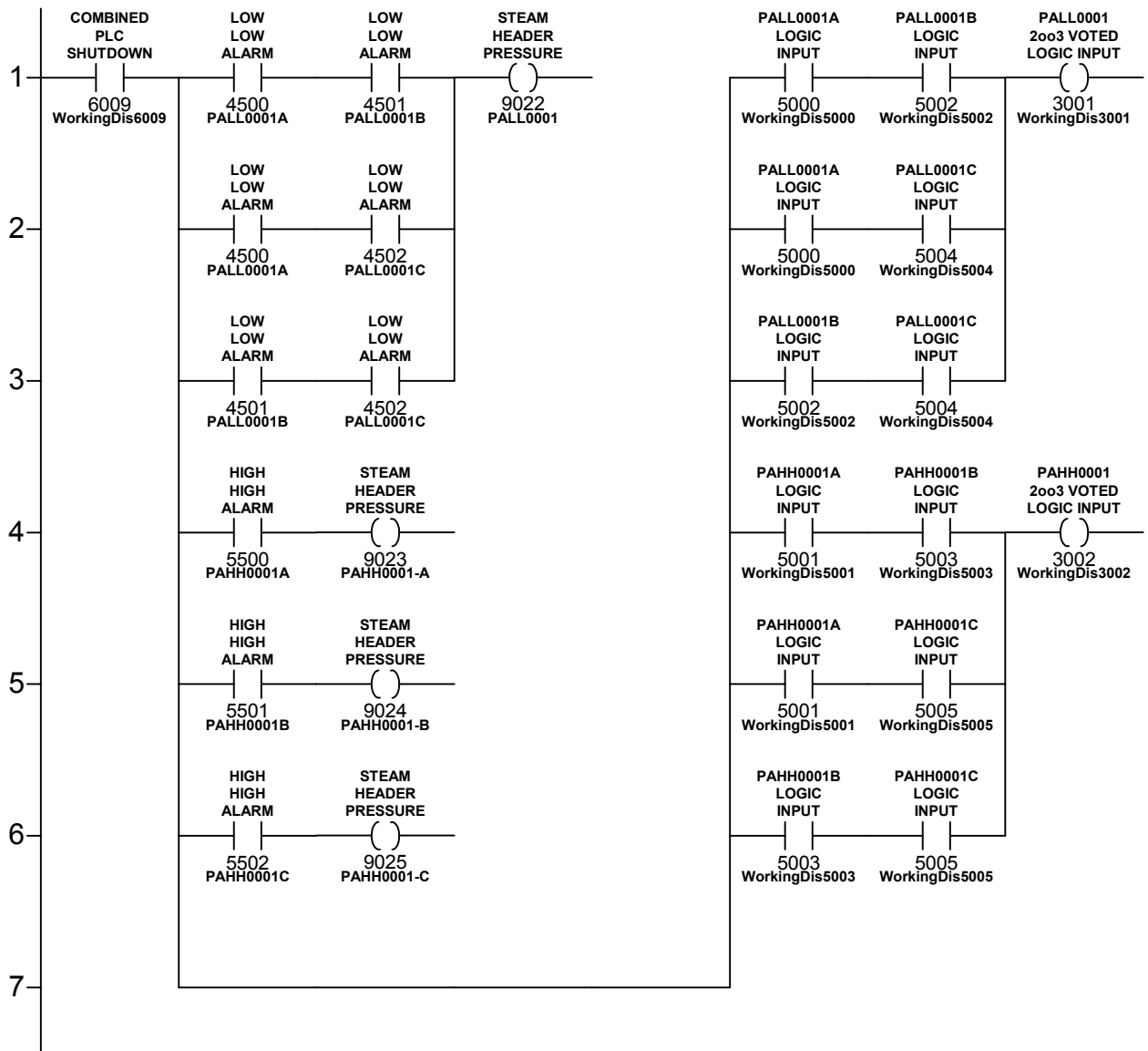


If safety critical analogue inputs are used, the alarm logic generated must include fail safe logic. This is Mandatory. A number of methods are available to generate fail safe digital logic inputs from analogue inputs, an example utilising DEAD BAND elements is given above (The fault discretes used are those given in the default Analogue test configuration). The example above is for a single channel with both high 3800 and low 900 alarms.

The above circuit includes user configurable hysteresis on the alarm values (set in example to 20 bits) and allows for up to 2 analogue alarm levels to be processed on a single network. Alarm status is configured to be identical to digital alarm status i.e. Logic 1 Normal, Logic 0 Alarm.

Alarm annunciation is independent of the fail safe logic input.

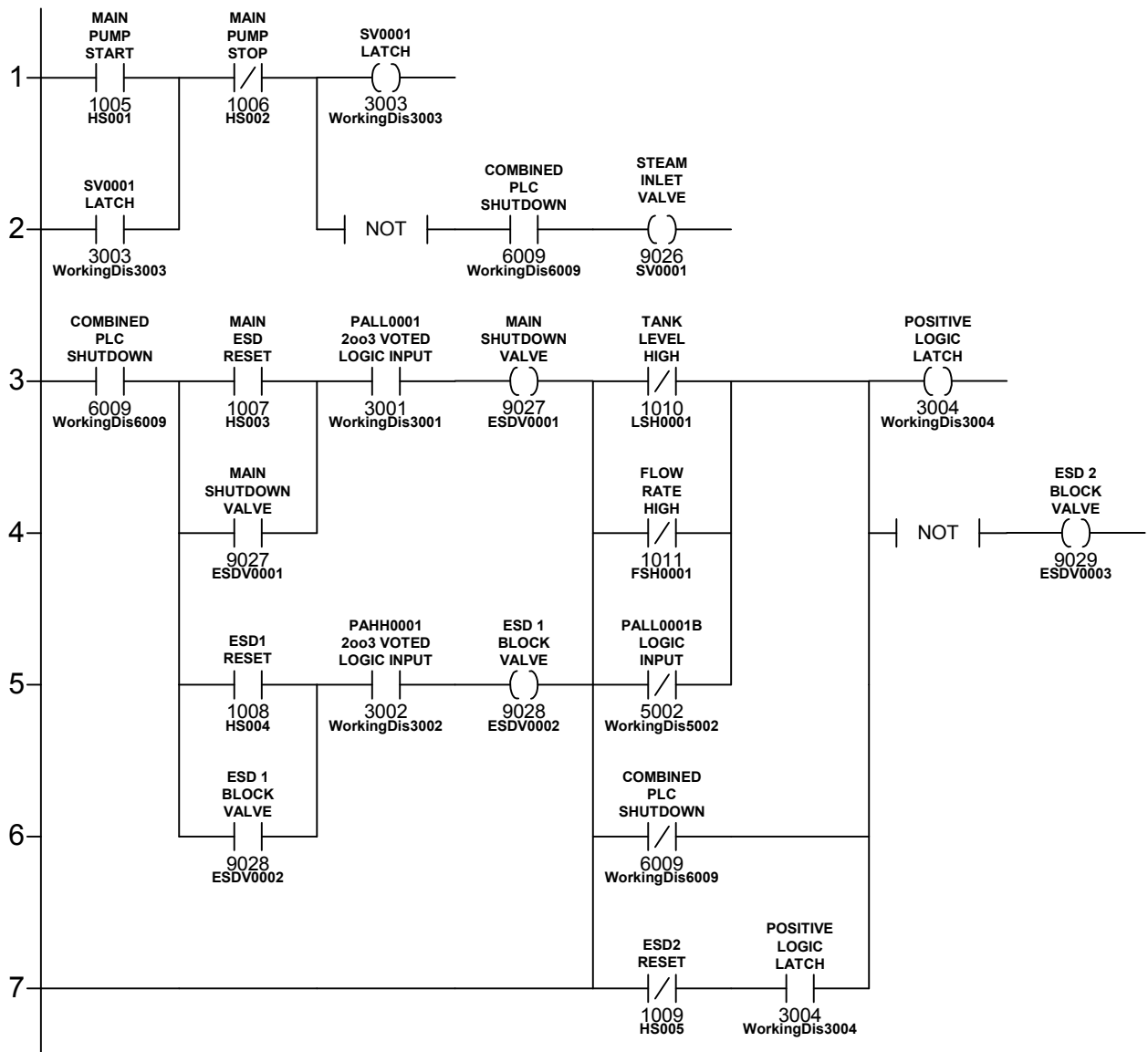
If 2 faults are diagnosed on an analogue input channel the module is marked as bad and the analogue input is given a negative value 8000H. This condition gives an O/C fault and trips the fail safe logic.



Example Analogue alarm annunciation - the non fail safe logic outputs should be used.

Example 2oo3 Voting for Logic Input using the fail safe alarms.

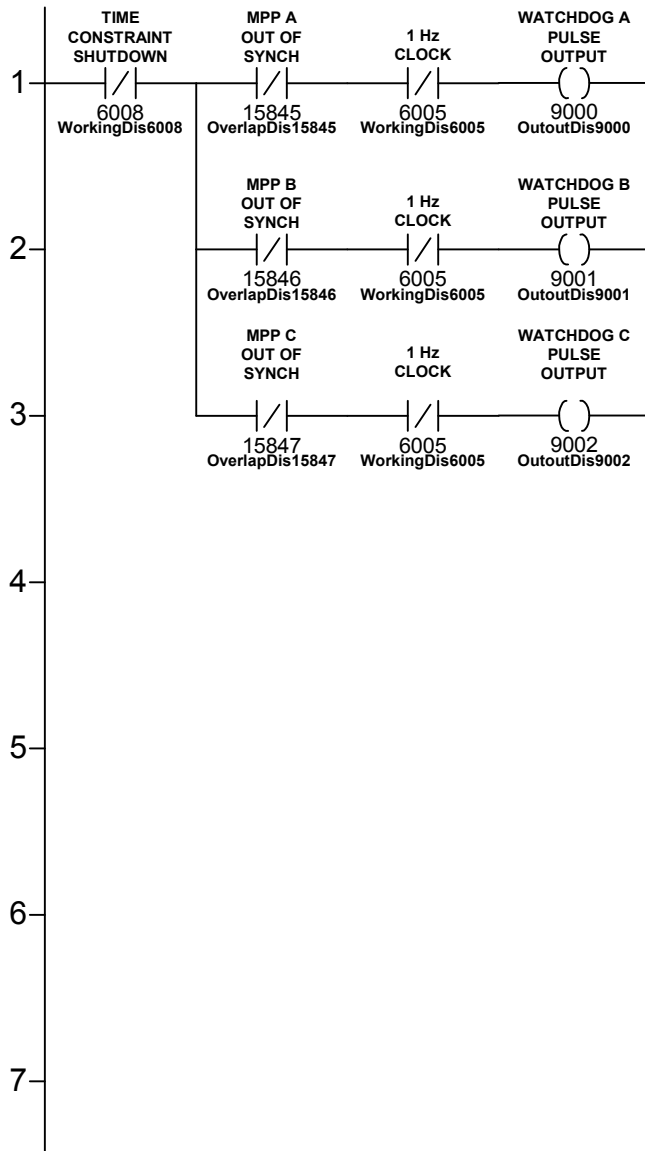
The Analogue fault conditions should also be separately annunciated e.g. Printer Messages or other serial outputs.



Example Shutdown Logic with resets are shown (both positive and negative logic example are shown). Implementation of Logic is to customer Cause & Effects/Logic Diagrams or other design documentation.

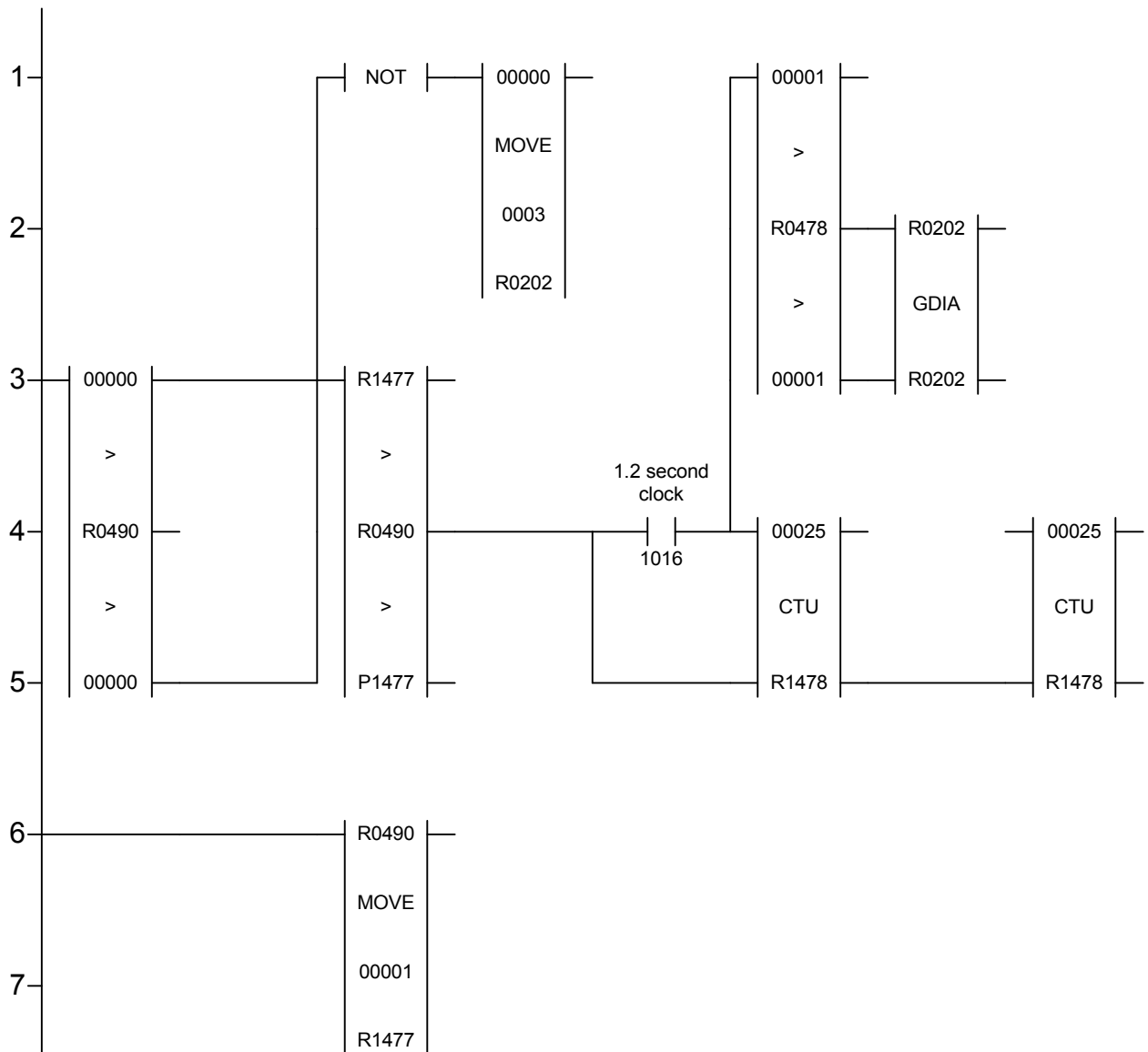
It is Mandatory that the diagnostic shutdown is included into the customers logic requirements such that all safety outputs are de-energised and the ESD logic is tripped (via discrete 6009) if only one processor is running, or the scan is the first scan, or the system time constraint is exceeded, or an critical I/O module is Off-Line for more than the time set in timer R1203, or an I/O module is removed from the chassis without first being taken Off-line, or a I/O chassis is lost to be system by total power failure or loss of two MBB modules.

In addition, only the fail safe logic input should be used for safety critical logics.



The triplicated watchdog module outputs are pulsed every 1 second provided that the system time constraint has not been exceeded and that the associated MPP module is not out of synch (stopped).

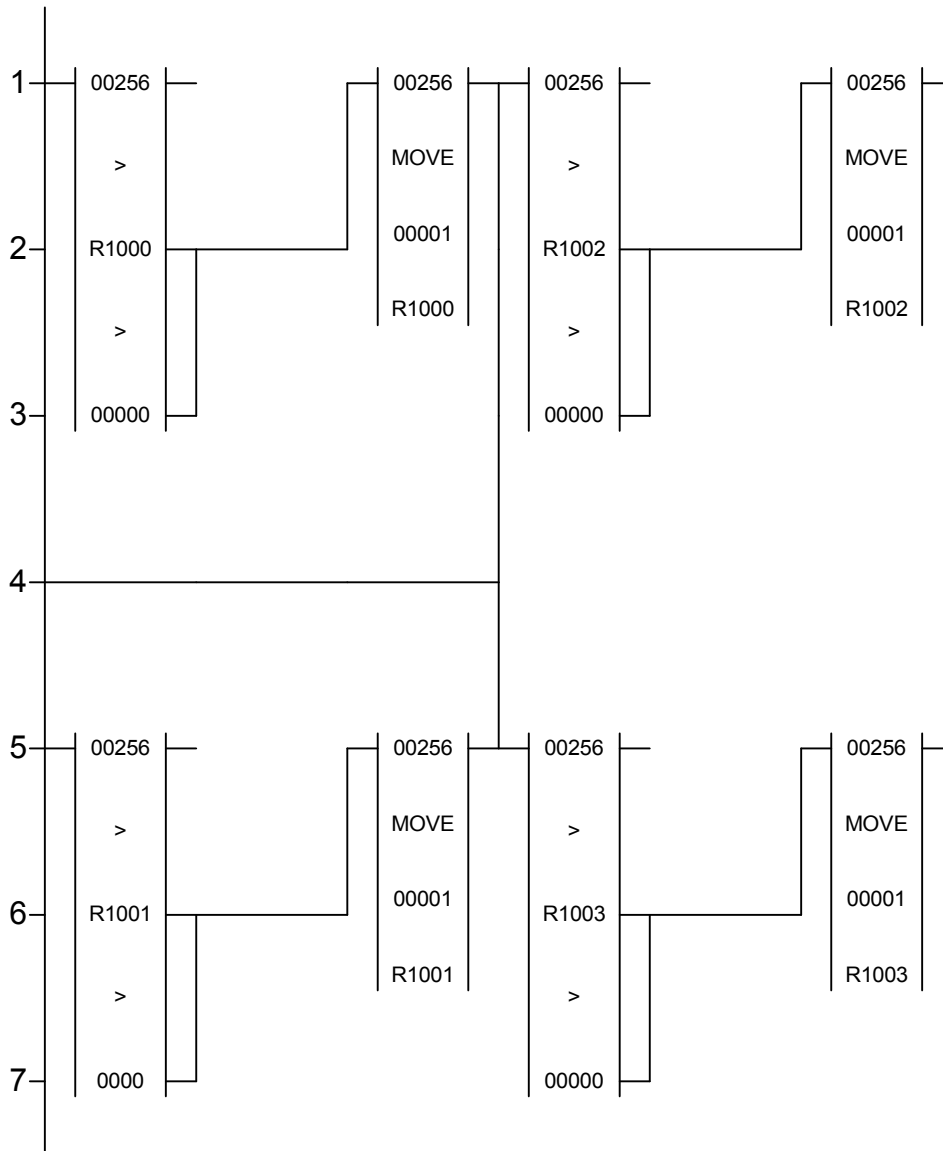
This is Mandatory Logic and must be placed in the last ladder network.



If the fault status is non-zero and not changing, then the GDIA element is called every 30 seconds (25x1.2 secs). The fault bits returned by GDIA are packed into one register per chassis.

If the Fault status is zero, then the chassis diagnostics are cleared, the number of registers being equal to the number of chassis in the system.

If the fault status is non-zero, but does change, then the 30 second timer is reset so that the GDIA element will be called 1.2 seconds after it has become stable.



The dead band element and the move function are mandatory to ensure that the analogue outputs are not driven below 256 decimal which will result in the module losing health. The value in the move element may be modified to higher value to prevent the output being driven below some minimum value example 4 mA = 895.

A similar network may be used to prevent the output being driven above a fixed value example 20mA = 3455.

9 Appendix 2 - Time Constraint Table (Low Demand of operation)

The following tables detail the actual time constraint time that is required for a certified system dependant on the maximum number of Safety loop outputs (SIL level 1 to 3) used on a single output module with.

9.1 Admissible Repair Times in hours for Low Demand Mode of Operation

Number of Safety Loops	SIL 1	SIL 2	SIL 3
1	63718	20149	6372
2	58062	18361	5806
3	53686	16977	5369
4	50170	15865	5017
5	47266	14947	4727
6	44813	14171	4481
7	42707	13505	4271
8	40872	12925	4087
9	39256	12414	3926
10	37816	11959	3782
11	36525	11550	3652
12	35357	11181	3536
13	34295	10845	3429
14	33323	10538	3332
15	32429	10255	3243
16	31603	9994	3160
17	30838	9752	3084
18	30125	9526	3013
19	29460	9316	2946
20	28837	9119	2884
21	28252	8934	2825
22	27701	8760	2770
23	27181	8595	2718
24	26689	8440	2669
25	26223	8293	2622
26	25781	8153	2578
27	25360	8020	2536
28	24960	7893	2496
29	24577	7772	2458
30	24212	7657	2421
31	23863	7546	2386
32	23528	7440	2353

10 Appendix 3 - Approved RTTS Versions

8.30-001 SC300E Operating system
 Identified
 Version 8.30 LOC SC-300E ROM System-001 Generated 5-MAR-1999 17:16
 Checksum
U86 - 702Dh
U106 - F854h
U87 - D04Fh
U107 - 026Dh

8.30-003 SC300E Operating system
 Identified
 Version 8.30 LOC SC-300E ROM System-003 Generated 21-Oct-1999 07:59
 Checksum
U86 - 7045h
U106 - F852h
U87 - D05Fh
U107 - 0273h

8.30-005 SC300E Operating system Identified
 Version 8.30 LOC SC-300E ROM System-005 Generated 19-May-2000 11:07
 Checksum
U86 - 486Eh
U106 - 0BC0h
U87 - 46ACh
U107 - 3E43h

8.30-006 SC300E Operating system
 Identified
 Version 8.30 LOC SC-300E ROM System-006 Generated 12-Jul-2000 15:38
 Checksum
U86 - 4885h
U106 - 0BCFh
U87 - 469Fh
U107 - 3D53h

8.30-007 SC300E Operation System
 Identified
 Version 8.30 REM SC-300E ROM System-007 Generated 04-May-2001 12:24

IC	Part No.	Checksum
U86	006-1372-31	D19F
U87	006-1373-31	285E
U106	006-1374-31	7697
U107	006-1375-31	0383

11 Appendix 4 - RTTS versions 8.30-005 and later versions

11.1 System Error Flags for RTTS version 8.30-005 and later versions

The following diagnostic flags are available from the 'FALT' call and can be incorporated in the system application logic to drive local alarm indicators and be transmitted to other systems or workstations.

Bit	Reference	Description
0	History	Entry in history table - errors logged relating to processors and communications
1	Data/Voting	2oo3 voting error – voting discrepancies encountered and logged by the processors during I/O scanning
2	LFD	latent fault detection of failed on or failed off signal paths – monitor and fault bits set depending on fault type and location
3	Monitor	Initialisation error – bits are set in the fault or monitor registers
4	INIT	System initialisation error – modules referenced in the table of operations are missing. Either a single slot module or both modules missing/offline in a dual slot hot repair partnership.
5	MPP A	Processor A failure – out of synchronisation
6	MPP B	Processor B failure – out of synchronisation
7	MPP C	Processor C failure – out of synchronisation
8	MPP A power	Processor A loss of power – fuse or PSU
9	MPP B power	Processor B loss of power – fuse or PSU
10	MPP C power	Processor C loss of power – fuse or PSU
11	MPP low Battery	Memory battery - low charge on one or more of the processor's batteries
12	Off-line module	Single slot repair - module off-line – should be on-line.
13	Global Output	Fault on any output module(s)
14	Multiple fault	Multiple faults on a module
15	Reserved	

Table 6 FALT flags RTTS 8.30-005 and later

FALT bit 4 - Initialisation error can be cleared when both modules or the only module of a hot repair partnership are installed in the chassis but are off-line. The application may be restarted when this flag is cleared by use of the Clear History command with the modules off-line. Whenever the initialisation flag is set, after all corrective actions have been taken to repair a SC300E system, the Configuration Report MUST be inspected for off-line modules prior to clearing the history table and restarting the application.

FALT Bit 13 - Global Output fault - this bit indicates that there is an error with at least one output module (Piano, AO or DO) in the system.

11.2 MHB44IND 4 channels pulse input and 4 channel analogue output module.

The Piano module may only be used with TriBuild for Windows version 1.42 and RTTS 8.3-006 or above with the following restrictions.

1. The registers used for the analogue outputs must be initialised to 256 or greater to prevent the module losing health.
2. The ladders for the analogue outputs must be configured to prevent the output registers going below 256 resulting in the module losing health.

11.3 MAO04IND 4 channel analogue output module.

The following conditions must be applied when using the analogue output module

1. The registers used for the analogue outputs must be initialised to 256 or greater to prevent the module losing health.
2. The ladders for the analogue outputs must be configured to prevent the output registers going below 256 resulting in the module losing health.

11.4 System identification

Both RTTS 8.30 versions are identified by the title in the history report and by the check sums of the EPROM's as follows:

11.4.1 SC300E RTTS 8.30-005

Version 8.30 LOC SC-300E ROM System-005 Generated 19-May-2000 11:07

U86	-	486Eh
U106	-	0BC0h
U87	-	46ACh
U107	-	3E43h

11.4.2 SC300E RTTS 8.30-006

Version 8.30 LOC SC-300E ROM System-006 Generated 12-Jul-2000 15:38

U86	-	4885h
U106	-	0BCFh
U87	-	469Fh
U107	-	3D53h

12 Appendix 5 – RTTS 8.30-007 and 008

12.1 System Identification RTTS 8.30-007

Version 8.30 REM SC-300E ROM System-007 Generated 04-May-2001 12:24

RTTS 8.30/007 is stored in PVCS Version Manager archives using the version label “Version 8.30-007”. The part numbers and checksums for the RTTS EPROMs are:

IC	Part No.	Checksum
U86	006-1372-31	D19F
U87	006-1373-31	285E
U106	006-1374-31	7697
U107	006-1375-31	0383

12.2 Change History

Support for Remote chassis added.

For full change history see PRN RTTS 8.30-007 Release Notes.

12.3 System Identification RTTS 8.30-008

Version 8.30 REM SC-300E ROM System-008 Generated 28-Aug-2003 11:27

RTTS 8.30/008 is stored in PVCS Version Manager archives using the version label “Version 8.30-008”. The part numbers and checksums for the RTTS EPROMs are:

IC	Part No.	Checksum
U86	006-1372-33	3176
U87	006-1373-33	89A9
U106	006-1374-33	7245
U107	006-1375-33	B9D8

12.4 Change History

Support for auto restart and channel error filters added.

For full change history see PRN RTTS 8.30-008 Release Notes.

13 Appendix 6 - TUV Approved Part Numbers and Revisions

13.1 Hardware Approvals.

Triguard SC300E – Hardware Components	Model No	Part No	Certification		
			AK5/6	SIL	EN 54
Chassis	Chassis	001-1109-01	✓	3	✓
Chassis Power Supply - 110/230Vac	PAC	031-1053-05-02	✓	3	✓
Chassis Power Supply - 24Vdc	PDC24	031-1054-04-02	✓	3	✓
System Modules					
Processor Module	MPP	001-1111-03-08	✓	3	✓
Processor Module	MPP	001-1111-04-00	✓	3	✓
Processor Module	MPP	001-1111-05-00	✓	3	✓
Processor Module	MPP	001-1111-06-04	✓	3	✓
Bus Buffer Module	MBB	001-1116-08-00	✓	3	✓
Serial communications module - 4 port - RS232	MSR04XI	001-1103-04-00	I/F		✓
Remote Bus Extender – Slave ++	MRB01XS	001-1130-04-00	✓	3	✓
Remote Bus Extender – Master ++	MRB04XM	001-1129-04-00	✓	3	✓
++ supported in RTTS 8.30-007 and above					
Digital Input and Output Modules					
32 channel analogue input module, isolated - 0/20mA	MAI32NAD	001-1145-02-00	✓	3	✓
32 channel analogue input module, isolated - 0/40mA	MAI32PAD	001-1147-02-00	✓	3	✓
32 channel analogue input module, isolated - 0/5Vdc	MAI32LAD	001-1113-05-00	✓	3	✓
32 channel analogue input module, isolated - 0/10Vdc	MAI32MAD	001-1143-04-00	✓	3	✓
4 channel analogue output module	MAO04NND	001-1180-02-02	I/F		
32 channel digital input module - 24Vdc	MDI32BIS	001-1104-05-05	✓	3	✓
32 channel digital input module - 24Vdc	MDI32BIS	001-1104-07-02	✓	3	✓
32 channel digital input module - 120V AC/DC	MDI32FIS	001-1157-01-04	✓	3	✓
32 channel digital input module - 120V AC/DC	MDI32FIS	001-1157-01-05	✓	3	✓
32 channel digital input module - 48Vdc	MDI32GIS	001-1195-00-02	✓	3	

Triguard SC300E – Hardware Components	Model No	Part No	Certification		
			AK5/6	SIL	EN 54
32 channel digital input module - 48Vdc	MDI32GIS	001-1195-00-03	✓	3	
64 channel digital input module, simplex - 24Vdc	MDI64BNS	001-1137-04-00	I/F		✓
64 channel digital input module, simplex - 24Vdc	MDI64BNS	001-1137-04-05	I/F		✓
16 channel digital output module, Supervised - 120V DC **dc only revision of 1160-3	MDO16DNS	001-1197-01-00	✓	3	
16 channel digital output module, Supervised - 120V AC/DC	MDO16FNS	001-1160-02-10	I/F		
16 channel digital output module, Supervised - 120V DC only ** now MDO16DNS	MDO16FNS	001-1160-03-01	✓	3	✓
16 channel digital output module, Supervised - 48Vdc	MDO16GNS	001-1193-00-01	✓	3	
32 channel digital output module, Supervised - 24Vdc	MDO32BNS	001-1112-03-13	✓	3	✓
32 channel digital output module, Supervised - 24Vdc	MDO32BNS	001-1112-04-00	✓	3	✓
4 Channel pulse input and 4 Channel analogue output module	MHB44IND	001-1118-02-02	I/F		
Termination Cards - Analogue Input					
16 channel analogue input, DIN to screw terminals - external power	TAI16AEA	099-1278-03-01	✓		
16 channel analogue input, DIN to screw terminals - external power	TAI16AEC	099-1332-01-01			
16 channel analogue input, DIN to screw terminals (250 Ohms) - external power	TAI16AER	099-1333-02-00	✓	3	✓
16 channel analogue input, DIN to screw terminals internal power	TAI16AIC	099-1277-03-01			
16 channel analogue input, DIN to screw terminals - line monitored, internal power	TAI16AIL	099-1307-02-02	✓	3	✓
16 channel analogue input, DIN to screw terminals (250 Ohms) - internal power	TAI16AIR	099-1310-03-00	✓	3	✓
16 channel analogue input, DIN to DIN - external power	TAI16BEC	099-1329-01-01			
16 channel analogue input, DIN to DIN - external power	TAI16BER	099-1344-02-00			
16 channel analogue input, DIN to DIN - internal power	TAI16BIC	099-1276-03-01			
16 channel analogue input, DIN to DIN - line monitored	TAI16BIL	099-1308-00-01	✓	3	✓
16 channel analogue input, DIN to DIN (250 Ohms) - internal power	TAI16BIR	099-1311-02-00	✓	3	✓
16 channel analogue input, DIN to ELCO - external power	TAI16EEC	099-1330-01-01			
16 channel analogue input, DIN to ELCO - external power	TAI16EER	099-1335-02-00			
16 channel analogue input, DIN to ELCO - internal power	TAI16EIC	099-1275-03-01			
16 channel analogue input, DIN to ELCO - internal power	TAI16EIL	099-1309-00-01			
16 channel analogue input, DIN to ELCO - internal power	TAI16EIR	099-1312-02-00			
Termination Cards - Digital Input					
16 channel digital input, DIN to screw terminals - external power - 24Vdc	TDI16AEA	099-1319-01-01			
16 channel digital input, DIN to screw terminals - internal power - 24Vdc	TDI16AIA	099-1257-03-00	✓	3	✓
16 channel digital input, DIN to screw terminals – internal power - 48Vdc ** future release	TDI16AIE	099-1409-00-00			

Triguard SC300E – Hardware Components	Model No	Part No	Certification		
			AK5/6	SIL	EN 54
16 channel digital input, DIN to screw terminals- internal power - 24Vdc	TDI16AIG	099-1400-00-00			
16 channel digital input, DIN to screw terminals - internal power 120Vac/dc	TDI16AIB	099-1326-01-00	✓	3	✓
16 channel digital input, DIN to screw terminals – Internal power – 24Vdc	TDI16AIJ	099-1402-00-00			
16 channel digital input, DIN to DIN – external power - 24Vdc	TDI16BEA	099-1320-01-01			✓
32 channel digital input, DIN to DIN – internal power - 24Vdc	TDI16BIA	099-1258-02-01	✓	3	✓
16 channel digital input, DIN to ELCO – external power - 24Vdc	TDI16EEA	099-1321-01-00			✓
16 channel digital input, DIN to ELCO – internal power - 24Vdc	TDI16EIA	099-1274-01-00			✓
32 channel digital input, DIN to screw terminals - external power - 24Vdc	TDI32AEA	099-1322-01-00			
32 channel digital input, DIN to screw terminals - internal power - 24Vdc	TDI32AIA	099-1301-02-00	I/F		✓
32 channel digital input, DIN to DIN - external power - 24Vdc	TDI32BEA	099-1323-01-01			
32 channel digital input, DIN to DIN - internal power - 24Vdc	TDI32BIA	099-1302-02-00	I/F		✓
32 channel digital input, DIN to ELCO - external power - 24Vdc	TDI32EEA	099-1324-01-01			
32 channel digital input, DIN to ELCO - internal power - 24Vdc	TDI32EIA	099-1303-02-00			
Termination Cards - Digital Output					
16 channel digital output, DIN to screw terminals - v/f safety relays	TDO16AFF	099-1336-01-00	✓	3	✓
16 channel digital output, DIN to screw terminals – internal power - 24Vdc	TDO16AIA	099-1259-03-00			
16 channel digital output DIN to screw terminals – internal power 120Vac/dc	TDO16AIB	099-1272-01-02	I/F		
16 channel digital output, DIN to screw terminals - power relays	TDO16AID	099-1331-00-01			✓
16 channel digital output DIN to screw terminals – internal - 48Vdc ** future release	TDO16AIE	099- 1407-00-00			
16 channel digital output DIN to screw terminals – internal - 120Vdc ** future release	TDO16AIG	099-1402-00-00	✓	3	✓
16 channel digital output, DIN to screw terminals - internal power - 24Vdc	TDO16AIH	099-1398-00-00			
16 channel digital output, DIN to screw terminals – internal - 24Vdc ** future release	TDO16AIN	099-1338-03-00	✓	3	✓
16 channel digital output DIN to screw terminals – internal power - 24Vdc LM	TDO16AIX	099-1384-02-01			✓
16 channel digital output, DIN to DIN – internal power - 24Vdc	TDO16BIA	099-1260-02-01			
16 channel digital output, DIN to DIN - internal power - 24Vdc ** future release	TDO16BIN	099-1339-03-00	✓	3	✓
16 channel digital output, DIN to ELCO – internal power - 24Vdc	TDO16EIA	099-1273-02-01			
PIANO and Analogue Output Termination Cards					
4 channel pulse input and 4 channel analogue output termination card	TPH44AIC	099-1356-01-00	I/F		
Fire and Gas Termination Cards					
Fire and Gas Input Termination Card	TFI32CIA	099-1268-01-01			
Fire and Gas Output Termination Card	TFO16DIA	099-1271-03-02			

Triguard SC300E – Hardware Components	Model No	Part No	Certification		
			AK5/6	SIL	EN 54
DMX Display Cards					
64 channel display driver - daughterboard (single)	TM117-DMxD/B	099-1035-07-01	I/F		✓
64 channel display driver - motherboard (single/dual)	TM117-DMxM/B	099-1048-05-01	I/F		✓
Triplicated Watchdog Timer					
Triplicated Watchdog Timer comprising	TWT10XZO	001-1187-01-00	✓	3	✓
Motherboard		099-1382-01	✓	3	✓
Daughterboard		099-1383-01	✓	3	✓
Miscellaneous Items					
Common Interface	CI	091-1004-03-00	✓	3	✓
Power distribution panel 24Vdc - 48 power points	PDD24	031-1055-01-02	I/F		✓
Bus expansion adaptor	TBA	061-1000-02	I/F		✓
Bus Termination Adaptor	TBT	001-1191-00-00	I/F		✓
Hot repair adapter (each)	THR	099-1245-00-01	I/F		✓
Hot repair adapter (set of 2)	THR	061-1001-00-01	I/F		✓
Blanking Plates	ML	053-1070-00-00	I/F		✓

13.2 Software Approvals.

Triguard SC300E – Software Components	Model No	Version	Certification		
Software and Firmware			AK 5/6	SIL	EN54
RTTS Operating System 3-2-0	RTTS	8.30-007	✓	3	✓
RTTS Operating System 3-2-0	RTTS	8.30-008	✓	3	✓
TriBuild					
TriBuild SC300E Single User Application Software	TriBuild	TriBuild V1.42	not S/R		✓
TriBuild SC300E Single User Application Software	TriBuild	TriBuild V1.43	not S/R		✓
TriLog					
Trilog	Trilog	V 2.2	Not S/R		
TriBuild – TUV approved modules for use in ESD applications	Module name	Version			
Analog alarm processing	analog.a86	1.2	✓	3	✓
Analog alarm processing	analog.a86	1.3	✓	3	✓
(always used)	cmpcrtts.a86	1.01	✓	3	✓
First-up Alarm Processing	fla.a86	1.1	✓	3	✓
Event processing	events.a86	1.4	✓	3	✓
Ladder element library (always used)	ladder.lib	5.43	✓	3	✓
Ladder element library (always used)	ladder.lib	5.44	✓	3	✓
Ladder element library (always used)	ladder.lib	5.45	✓	3	✓
Large RTTS (always used)	largrtts.lib	1.01	✓	3	✓
No Tridac (always used)	notridac.p86	1.0	✓	3	✓
PID control blocks (certain elements)	pidblks.lib	5.34	✓	3	✓
PID control blocks (certain elements)	pidblks.lib	5.35	✓	3	✓
System Configuration	syscon.a86	1.4	✓	3	✓
Triguard protocol (peer to peer)	tgprot.lib	3.21	✓	3	✓
TI protocol (mandatory but not to be used)	tiprot.a86	5.31	✓	3	✓
Network compiler	trigardc.lib	5.33	✓	3	✓
Utilities	utils.a86	1.5	✓	3	✓
Fire & Gas Modules approved for EN 54					
DMX driver	dmxdrive.a86	1.0			✓

Triguard SC300E – Software Components	Model No	Version	Certification		
Software and Firmware			AK 5/6	SIL	EN54
Halon	halonb.a86	1.0			✓
Halon	Hanolh.a86	1.0			✓
Halon	Halonl.a86	1.0			✓
Lamp test	Lmptest.a86	1.1			✓
N of M alarm	Nofmalm.a86	1.1			✓
N of M alarm X	Nofmalmx.a86	1.1			✓
Status	Stausb.a86	1.0			✓
Status	Staush.a86	1.0			✓
Status	Stausl.a86	1.0			✓
MODBUS					
Modbus slave RTU protocol	modrtu.p86	1.3	✓	3	✓
Stand alone modules					
Discrete mapping	dismap.a86	1.1	✓	3	✓
Time synchronisation	Timesync.a86	1.4	✓	3	✓
Programmed Devices					
MBB					
MBB FPGA		006-1435-04	✓	3	✓
Common Interface					
Common Interface Firmware	V2.01	006-1322-05	✓	3	✓
Common Interface Firmware	V2.02	006-1322-06	✓	3	✓
Common Interface Firmware	V2.04	006-1322-07	✓	3	✓
CI FPGA		006-1477-01	✓		
CI FPGA		006-1477-02	✓	3	✓
MSR04XI					
FPGA	U14	006-1354-00	I/F		✓
Quad serial I/O firmware V1.02	U21	006-1355-03	I/F		✓
Quad serial I/O firmware V1.02	U26	006-1356-03	I/F		✓
Quad serial I/O firmware V1.03	U21	006-1355-04	I/F		✓
Quad serial I/O firmware V1.03	U26	006-1356-04	I/F		✓
Daughter board		099-1240-00	I/F		✓
MPP					

Triguard SC300E – Software Components	Model No	Version	Certification		
Software and Firmware			AK 5/6	SIL	EN54
RTC 3-2-1	U32	006-1371-01	✓	3	✓
RTC 3-2-1	U32	006-1371-02	✓	3	✓
MRB01XS					
Firmware	U5	006-1543-02	✓	3	✓
MRB04XM					
Firmware	U22	006-1542-01	✓	3	✓