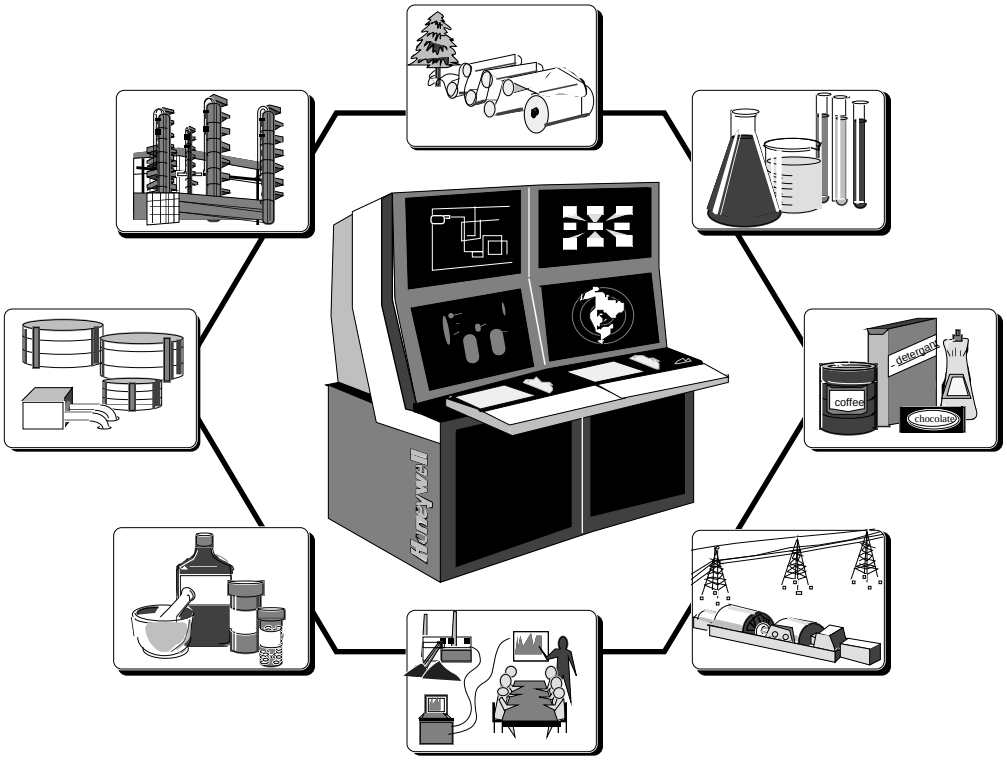
Honeywell

TDC3000X Safety Manager Triconex TRICON Specification and Technical Data

SM03-500
1/96



Total Plant

TDC 3000^X
Safety Manager Module for Triconex TRICON™ Version 8 Controller
Specification and Technical Data

TABLE OF CONTENTS **Page**

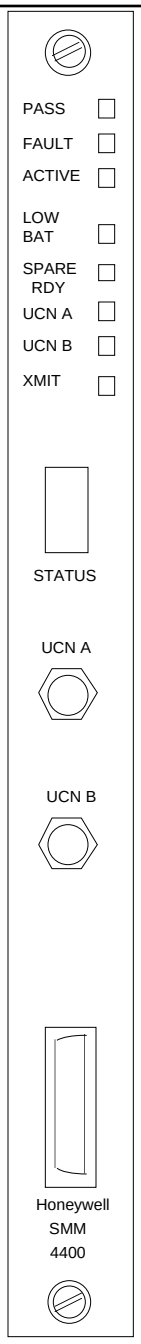


Figure 1 — Safety Manager Module

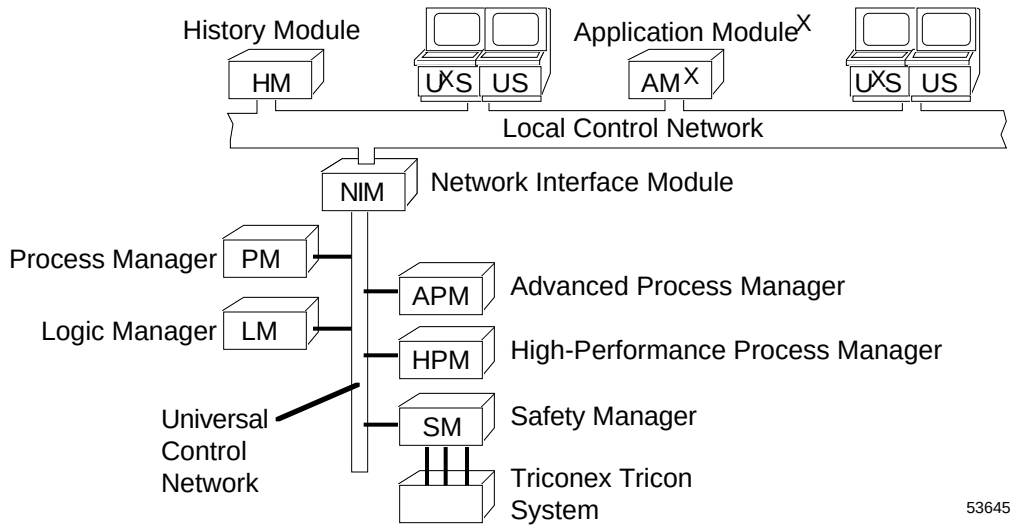


Figure 2 — TDC 3000X Architecture

Introduction

The term Safety Manager (SM) refers to a class of nodes on the Universal Control Network (UCN) that allows integration of safety systems to the UCN. One of these SMs is the Release 500 TRICON™ Safety Manager that provides a Triple Modular Redundant (TMR) fault-tolerant controller for safety and shutdown applications on the TDC 3000X UCN; it consist of a Triconex TRICON™ Version 8 controller and an R500 Honeywell Safety Manager Module (SMM) interface card. Another one of these SMs is the Release 510 FSC Safety Manager that provides a dual redundant fault-tolerant controller for safety and shutdown applications on the TDC 3000X UCN; it consists of a Honeywell Fail Safe Controller (FSC) system a an R510 Honeywell SMM interface card.

The specification and the technical data contained in this document, for the most part, concerns the R500 SMM for Triconex TRICON™ Version 8 Controller which will be referred to in the remainder of this document as SMM. The Triconex TRICON™ Version 8 controller will be referred to in the remainder of this document as TRICON™. For detailed specifications and technical data on the Triconex TRICON™ system, please refer to Triconex documentation.

In keeping with Honeywell's philosophy of consistent product evolution, the Safety Manager adds yet another increment of power to the TDC 3000X advanced system for industrial control. Now TMR logic functions are integrated into the architecture of the Universal Control Network to support integrated operations and control. The result is a true TDC-based window into this powerful safety system that has superior uptime and safety-related performance for applications such as:

- Emergency Safety Shutdown (ESD) in refineries, petrochemical/chemical plants, and other industrial processes
- Boiler Flame Safety
- Turbine Control Systems
- Offshore Fire & Gas Protection

Because of its integration into the Universal Control Network, as shown in Figure 2, the Safety Manager shares some of the same important features as its UCN peers. This includes:

- Direct peer-to-peer communication with other Safety Managers, Process Managers, Advanced Process Managers, High-Performance Process Managers, and Logic Managers (initiated by either an SM, PM, APM, HPM, or LM).
- Communication with operators, engineers, and maintenance personnel at the Universal Stations, UXSs, and Universal Work Stations.
- Support of higher level strategies through communication with Application Modules and host computers on the Local Control Network.
- Database restoration of the Safety Manager Module from the History Module.

Universal Control Network

The communications channel for the High-Performance Process Manager is a local area network called the Universal Control

Network (UCN). Introduced to TDC 3000^X users in 1988, the UCN is the secure path for process I/O connections to the TDC 3000^X.

The UCN features a 5 megabit per second, carrier band communication system with a token bus network. It is designed to be compatible with IEEE* and ISO** standards. UCN communications are consistent with the growth and direction of evolving international standards, with appropriate Honeywell extensions for secure process control applications.

The UCN uses redundant coaxial cables and can support up to 32 redundant devices. The UCN supports peer-to-peer communication between devices on this network. This feature enables sharing information among HPMs, APMs, PMs, Safety Managers, and Logic Managers on the network, thus offering tremendous power and flexibility in implementing advanced, coordinated, control strategies.

Network Interface Module

The Network Interface Module (NIM) provides the link between the Local Control Network and the Universal Control Network. Accordingly, it makes the transition from the transmission technique and protocol of the Local Control Network to the transmission technique and protocol of the Universal Control Network. The NIM provides LCN module access to data from UCN-resident devices. It supports program and database loads to the Safety Manager and forwards alarms and messages from the network devices to the LCN. The NIM is also available in a redundant configuration to provide automatic continued operation in the event of a primary failure.

* Institute of Electrical and Electronics Engineers
** International Standards Organization

LCN time and UCN time are synchronized by the NIM. The NIM broadcasts LCN time over the UCN.

The SM (as well as HPM and APM) uses it for all alarm (event) timestamping and for DI SOE (sequence of events) time synchronization.

Functional Description

Functional Overview

The primary function of the Safety Manger is to provide a Triconex TRICON™ interface to the TDC via a direct connection to the UCN while at the same time provide the ability to isolate ESD (Emergency Shutdown) functions from process control strategies on a separate "Safety Network." Its interface to the Universal Control Network enables the Safety Manager to readily share data with its peers, Process Managers, Advanced Process Managers, Logic Managers, as well as other Safety Managers. As shown in Figure 3, the SM consists of a communication processor, known as the Safety Manager Module (SMM) that serves as the UCN interface, and a Triconex TRICON™ system with its own I/O subsystem.

The Triconex TRICON™ processors read the process inputs and execute the user-written ladder logic program. Typical user's control programs execute at about 100 millisecond intervals. Input to output times vary based on the number of points, control program size, and type of points; and are usually 2 to 3 control program scans, or 200 to 300 milliseconds, for a 100 millisecond control program scan time. Inputs are polled by the Main Processors, processed by the control program, voted, and then transmitted to the output modules.

Operating on a scan cycle that is independent of the Triconex TRICON™ control processors ladder logic cycle, the SMM collects and processes information to and from the relay ladder logic.

The SMM converts this data to UCN data types (Tag.Parameter), performing engineering unit conversion, alarm handling, annunciation, diagnostic status reporting, and UCN communication functions. The normal SMM scan cycle is 1/2 second.
Operator changes from the Universal Station are written immediately to the SM/Triconex TRICON™ control processor only if all of the following conditions are met:

- The Safety Manager write protect flag is set to accept operator or peer-to-peer input
- The TRICON™ key switch is in "Program" or "Remote" setting
- Specific alias variables to be written to are defined in the TRICON™ control program as "Read/Write." (Alias variables are defined in the TRISTATION workstation Dictionary Editor, then downloaded to the TRICON™)

The Safety Manager Module database is configured from the Universal Station. Once loaded into the Safety Manager, this SMM configuration data can be saved on the History Module, and downloaded over the UCN to the SMM. The ladder logic program for the Triconex TRICON™ is developed using the Triconex TRISTATION workstation. Once loaded in the memory of the TRICON™ main processors, the control programs are saved in the TRISTATION database, which can save multiple ladder logic programs under separate file names. In addition to integration of Safety Manager data points into standard Universal Station operating displays, some additional displays are available for maintenance. Nearly all diagnostic information that is provided in the TRICON™ is available at the US.

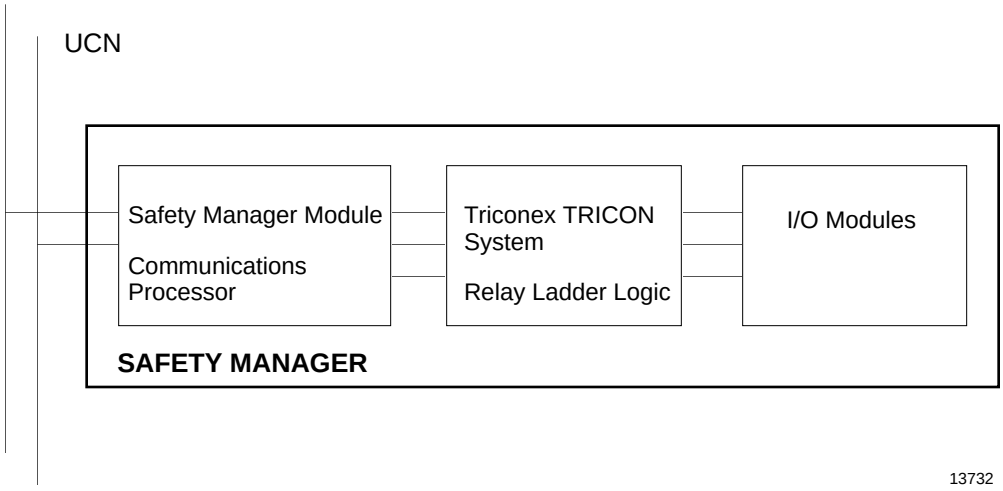


Figure 3 — Safety Manager Architecture

Data Point Types

Table 1 shows the SMM point types and their related maximum number of points per SMM. **Note:** The total maximum number of all points added together cannot be used with one SMM. A mixture of point types and their related load on the system must be considered by adding the total Processing Units (PU's) per Point so as not to exceed 6000.

This table applies uniquely to the Safety Manager Module. The user assigns these points to the field I/O points that are read and stored in the TRICON™ , and then translated to the SMM via Modbus alias ranges. In many cases, such as in Digital Composite points, multiple I/O points will be combined into a single SMM point for greater meaning on the operator display. Some field points will not require associated Safety Manager Module points; therefore, the number of different types of data points configured for the Safety Manager Module may differ from the actual number of I/O and memory points configured in the TRICON™ .

Digital Input: A Safety Manager Module digital input (DI) can be acquired from any designated DI status location within the TRICON™ memory. Typically, it would be mapped to an Input Status Table address that contains the status of a process connection.

Digital Output: Upon receipt of a digital output (DO) request from a system device, the SMM records the demanded status in its "current status table" and passes the status to the TRICON™ Control Processors to be written into its designated memory location. This is true only if the SMM "write protect flag" is set by the TRISTATION to accept DO status demands from a

Table 1 — Maximum Number of Each Data Point Type per SMM with PU Loading and Example

Point Type	Maximum #	PUs/Pt. @ 1/2 sec.
Analog Input	up to 1000	10.2
Analog Output	up to 1000	8.5
Digital Input	up to 2000	2.5
Digital Output	up to 2000	1.2
Digital Composite	up to 650	11.1
Timer	up to 1500	3.1
Linkage Point	up to 30	200.0
Flags	up to 2000	0
Numerics	up to 1000	0
Linkage Point fixed at 1/2 second scan.		

Safety Manager PU Loading				
Point Type	Scan Time sec.	PU/PT	PT. Qty	Total PUs
Analog Input	1.0	10.2	70	375
Analog Output	1.0	8.5	35	149
Digital Input	0.5	2.5	700	1750
Digital Output	0.5	1.2	350	420
Digital Composite	0.5	11.1	200	2220
Timer	0.5	3.1	30	93
Linkage Point	0.5	200.0	5	1000
SMM Total			1390	5989
Maximum Number				6000
Flags & Numerics not listed, since PU weights are 0.				

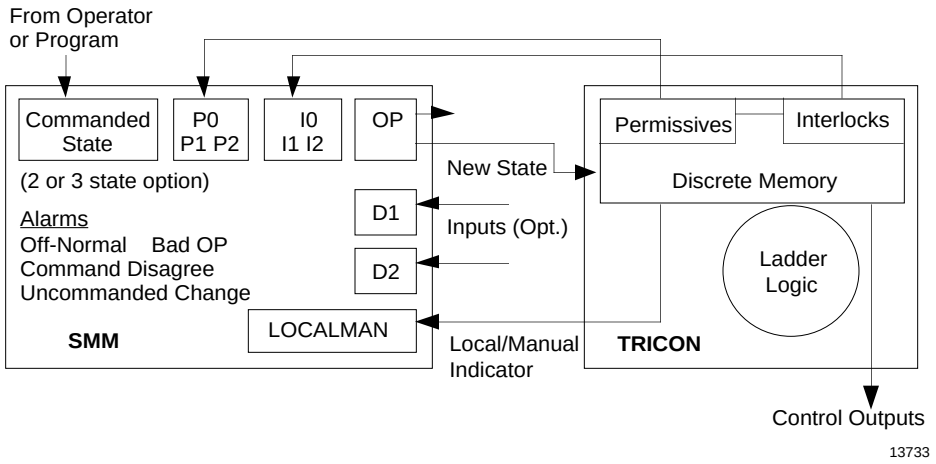


Figure 4 — Example Showing Digital Composite Point Data Flow

system device, the TRICON™ keyswitch is set to "Remote" or "Program", and the control program point is configured as "Read/Write". Upon receipt of the command, the TRICON™ returns an acknowledgment to the SMM for confirmation to the originator. After the write, the DO reverts to monitoring the TRICON™ value.

***Digital Composite**:* Digital composite (DC) points are multi-input/multi-output digital points used primarily for motors and valves. They provide an improved view of the process to the operator. They are primarily faceplates to display motor control functions implemented in the relay ladder logic program. Figure 4 shows a diagram representing the major parameters associated with this type of point. It shows how the commanded state is passed from the SMM to the TRICON™ , where it can be processed by the ladder logic program. Permissives and interlocks, if built into the TRICON™ logic, are communicated to the SMM, where they can influence the resulting output parameter (OP). Process feedback can be provided through one or two optional inputs (D1, D2). A local manual switch status can also be monitored to show if outputs are being controlled by the TRICON™ or by an external device.

***Analog Input**:* Engineering unit conversion and limit checking is performed on each of the analog input (AI) points. Alarms can be generated accordingly and there is a provision for alarm deadbands.

***Analog Outputs**:* An analog output (AO) from the UCN is converted by the SMM to the TRICON™ format, and then queued as a "write command" for the designated TRICON™ register. This will be processed during the next ladder logic scan. Again, this is only true if the SMM "write protect flag" is set by the TRISTATION to accept AO status demands from a system device. After the write command, the SMM reads the value from the TRICON™ register and returns it to the SMM database for history, logging, or operator inquiry.

***Linkage**:* The function of the linkage point in the SMM also referred to as the "logic point", is to transfer data between UCN and TRICON™ connections. Any pairing is acceptable, and can include discrete, unsigned integer, and real data formats. This point is the basis for the SMM application-level support of peer-to-peer communications on the UCN. Each linkage point can accommodate 12 input connections and 12 outputs. UCN connections are limited to a maximum of 50 inputs total and 50 writes per 0.5 second scan.

***Flag**:* A Flag point is a two-state (On/Off) point that is used for storing a Boolean value. Flag points are not scheduled and are not processed. Their state is changed from another function, such as by operator input or a user-written program. There may be up to 2000 flag points, the first 256 of which are considered to be in alarm when in the ON state.

Numeric: The numeric point provides for reading and writing of integer or real values, such as accumulations. There may be up to 1000 numeric points, and they can be optionally configured with a unique tag name.

***Timer**:* The timer point offers access to registers that are associated with relay ladder logic timers. The point controls the timer by writing to the Run Contact and Accumulator. Up to 1500 timer points can be processed, and full control of the timer by the operator is supported.

Alarm System Functions

The Safety Manager Module supports the extensive alarming features of TDC 3000^X. As process alarms are detected, they are brought to the operator's attention at the Universal Station through keyboard LEDs and a variety of displays, including alarm summaries, alarm annunciator displays, group displays, and custom graphic displays. Because alarms can be configured to selected areas or units, operators need not be subjected to alarms that do not relate to their specific assignments.

SMM analog inputs can be configured for High/Low alarm detection with a fixed deadband or engineering-unit deadband. Alarm messages include the "Alarm Limit Exceeded" indication. An analog input connected to another configured tag, such as a regulatory slot in a PM, can have its alarms assigned to that tag, thereby providing a single interface to the operator. SMM digital input points can be configured for "off-normal" alarms or for alarms triggered by a change in the process input state. Digital composite points provide for off-normal alarms for inputs. Where there are both inputs and outputs, Command Disagree alarms can be established. This provides for the situation where the actual state changes relative to the commanded state, as well as when the actual state fails to track the commanded state within a configurable time period.

Point Processing

All data being transferred between the SMM and the TRICON™ can be configured to be updated with either a 0.5 or 1 second scan cycle. The load limit of the SMM is 6000 processing units (PUs), each point type requires a different PU loading as shown in Table 1. All point types (except Linkage, Flag and Numeric) require 1/2 as much of the PU loading at 1 second as they require at 1/2 second. A second independent SMM (or a second set of redundant SMMs) can exist in the same TRICON™ main processor chassis to double the PUs from one TRICON™ system mentioned above. Actual ladder logic processing typically occurs at much faster rates. Operator output changes are processed immediately by the SMM and transferred to the TRICON™ only if the SMM "Write Protect Flag" is set to accept these output changes.

Peer-to-Peer Communications

The Safety Manager Module provides the ability to implement inter-node process control strategies between the SM and other UCN nodes, such as LM, PM, APM, HPM or another SM. These transactions are initiated via the **Linkage Point**. There are 12 enabled links per point and up to 30 points are permitted. There is a limit of 50 UCN input (fetch) connections and 50 UCN stores per SMM scan at the 0.5 second standard scan rate.

Write Protection

The SMM maintains safety and reliability of the TRICON™ safety system by providing multi-level protection against a "write" of control data through the interface. To provide for safety agency certification, "write" protect algorithms reside in the TRICON™ main processors and in the SMM personality. Universal Station operator and peer-to-peer writes are written immediately to the Triconex TRICON™ control processors only if each of the following conditions are met:

- Safety Manager write protect flag is set to enable writes
- TRICON™ key switch is in "Program" or "Remote" setting
- Specific alias variable to be written to is defined in the TRICON™ control program as "Read/Write". (Alias variables are defined in the TRISTATION workstation Dictionary Editor, then downloaded to the TRICON™ .)

There is a TRICON™ resident Write Protect Flag for each TRICON™ main chassis slot configured for an SMM, which is configured via the TRISTATION and is "read only" from the SMM. When set, SM blocks "write" requests. The SMM software will not allow any of its output points to be mapped to TRICON™ output aliases. Only memory aliases can be connected to DO, AO, DC, and Linkage Point outputs. Flag and Numeric Points can only be connected to input or memory aliases.

Displays

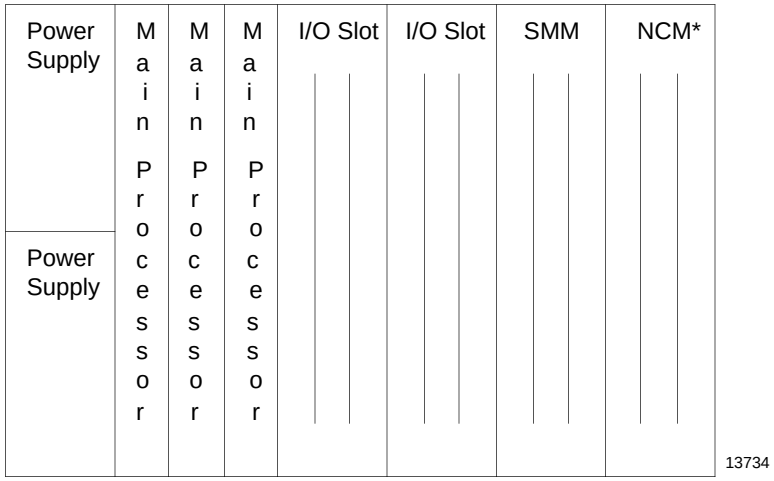
The U^{X}S displays this new UCN node as 'SM' on the UCN Status Display. Diagnostic displays emulate the Triconex TRISTATION chassis displays with the SM Overview Display showing all possible 15 racks of equipment information. Detail displays show individual rack displays. Displays show failure mode information to the board level.

Physical Characteristics

Standard Configuration

The standard configuration for a Safety Manager consists of:

- A Triconex TRICON™ version 8 main chassis with the following modules:
  - Honeywell Safety Manager Module
  - Dual power supplies
  - Three main processors
  - Network Communications Module (NCM) or Enhanced Intelligent Communication Module (EICM)



* A non-redundant NCM or EICM can be used

Figure 5 — Modules in Single Processor Card File

- One or more I/O cards and I/O expansion chassis
- Standard UCN cabinet(s) enclosing the above files

Processor Card File

Figure 5 illustrates typical module positions for a single Safety Manager main chassis. Two power supplies reside on the left side of all chassis, one above the other. In the Main Chassis, the three Main Processors are immediately to the right. The remainder of the main chassis is divided into four logical slots for I/O and Communication Modules. Each logical slot provides three physical spaces for modules. An I/O termination module belongs in the left-most physical space or, if a communication module is being used, a blank panel is placed here.

The middle physical space houses the primary I/O card or primary communication module. The right-most physical spaces house the hot spare I/O Module or the hot spare communication module. I/O cards or communication modules, such as the Safety Manager Module, can be assigned to any one of these logical slots. In addition to the SMM, a Triconex Network Communication Module is recommended for the TRISTATION configurator connection and also for multidrop Ethernet networking capability to other SMs. Up to 14 I/O expansion chassis, each housing up to 5 I/O logical slots, can be added to the main chassis. Triconex TRICON™ I/O cards are available in a number of different models to accommodate anywhere from 8 to 64 inputs or outputs per card. For more detailed information on the TRICON™ system, please refer to Triconex literature.

Options

Safety Manager Module Redundancy

As a standard feature, a Safety Manager Module uses dual redundant communication paths to the UCN. In addition, each SMM has triple redundant ports operating continuously to each of the triple redundant TRICON™ main processors via the TRICON™ communication bus. As a highly recommended option, dual redundant SMMs are available. The secondary SMM is synchronized (database copied) in less than one second over a private bus link and its switchover time is less than one second (writes to the primary are acknowledged after the secondary receives a copy of the request). The UCN acts as a backup to the slot bus for SMM backup.

Sequence of Events

The SMM provides Sequence of Events (SOE) for DI points with the information presented in the standard TDC 3000^X SOE displays and journals. The resolution of the event data is the scan time of the TRICON™ controller with the time stamp appended by the TRICON™ . Safety Manager time synchronization with the LCN is accomplished as follows: the NIM synchronizes with the LCN, the UCN nodes (e.g., SMM) synchronize with the NIM, the TRICON™ reports the TRICON™ time to the SMM, the SMM requests TRICON™ time correction.

The TRICON™ time stamps the digital input change-of-state events (all non-SOE events are time stamped by the SMM).

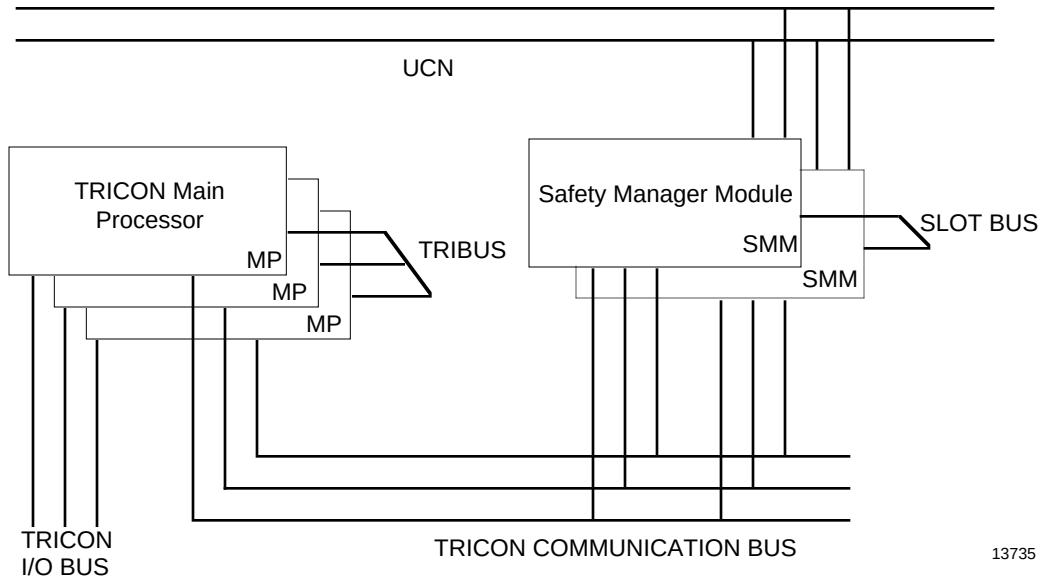


Figure 6 — SMM Redundancy

The SMM prioritizes the collection and distribution of non-SOE events over SOE events (such as alarms which need to be distributed over the UCN as quickly as possible) and it must regulate the distribution of events so that no more than 512 SOE events are sent over the UCN in any 10 second period.

The SM provides Event Recovery buffering for up to 2 events per point for up to 2000 points, or a total of 4000 events in a 20 second window.

The SM SOE does not interfere with the TRICON™ SER (Sequence of Events Recorder) option, and the sequence of events configuration is separate from alarm configuration.

The SM can ride through NIM and SMM failover without loss of SOE events. The SMM, on transition to RUN state after powerup and subsequent program load or memory retention, must command immediate Event Recovery (similar to the APM).

Note: It will wait for the first UCN Timesync before issuing the first SM Timesync and any SOE events collected during this period must receive a null time stamp.

Miscellaneous

System Requirements

The Honeywell TDC 3000^X system must be of a Release 500 or higher. The Triconex TRICON™ system must be of Version 8.

Model and Part Numbers

	Honeywell	Triconex
Single Safety Manager Module model number	MU-SMMS01	4400
Dual Redundant Safety Manager model number	MU-SMMR01	4400 (quantity 2)
Single Safety Manager Module part number	51309227-100	4400

SMM Specifications

Environmental Specifications	
Operating Temperature	0 to 60 degrees C, ambient
Storage Temperature	40 to 75 degrees C
Relative Humidity	5% to 95%, non-condensing
Vibration, Sinusoidal	2 G at 10 to 500 Hz
Shock	15G for 11 msec
Electrostatic Discharge	IEC 801-2, Level 3 (8KV)
Conducted Susceptibility	ANSI C37.90-1978, Surge Withstand IEC 801-4, Class 3, Fast Transient/Burst NEMA ECS2-230-4, Showering Arc MIL-STD-461C Part 4, per MIL-STD-462
Rated Susceptibility	IEC 801-3, Level 3/BS6667 Part 3, Level 3/SAMA MIL-STD-461C Part 4, per MIL-STD-462 Method RS01, Magnetic Field Method RS02, Induced Magnetic Field Method RS03, Electric Field IEC TC77B (Sec) 72, Magnetic Field
Conducted Emissions	Measured per MIL-STD-462/CISPR 11 & CISPR 22 Method CE03
Rated Emissions	Measured per MIL-STD-462/CISPR 11 & CISPR 22 Method RE02
"Ambient" refers to the air temperature measured at the bottom of the chassis	

International Standards & Safety Codes
TÜV Rheinland: Certified to fulfill the requirements of "Class 5" safety equipment as defined in the following documents: Din V VDE 19250, DIN V VDE 0801, DIN VDE 0116/10.89 Canadian Standards Association (CSA) - CSA certified to fulfill requirements of these two standards: CSA Standard C22.2 No. 0-M982 General Requirements - Canadian Electrical Code, Part II CSA Standard C22.2 No. 142-M1987 for Process Control Equipment Other Safety Agencies: Designed to comply with Underwriters Laboratories Inc. (UL) and Factory Mutual Research Corporation (FM).

Mechanical Specifications	
Overall dimensions	1" W x 14" H x 17" D
Approximate weight	4.3 lbs. (1.9 kg)

Copyright, Trademarks, and Notices

The following are trademarks of Honeywell Inc.:

TDC 3000^X system

The following are trademarks of their respective companies or organizations:

Triconex
Modbus

All other brand or product names appearing herein are trademarks of their respective companies or organizations.

While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a particular purpose and makes no express warranties except as may be stated in its written agreement with and for its customer.

In no event is Honeywell liable to anyone for any indirect, special or consequential damages. The information and specifications in this document are subject to change without notice.

Printed in U.S.A. — © Copyright 1996 - Honeywell Inc.