Honeywell

Safety Manager Module Implementation Guidelines

for use with the Triconex TRICON Version 8 systems

SM11-500

Total Plant®

Honeywell

Implementation
Safety Manager TRICON

Safety Manager Module Implementation Guidelines

for use with the Triconex TRICON Version 8 systems

SM11-500
4/96

Copyright, Notices, and Trademarks

Revision 03 – March 11, 1996

This document was prepared using Information Mapping® methodologies and formatting principles.

Honeywell
Industrial Automation and Control
Automation College
2820 West Kelton Lane
Phoenix, AZ 85023

(602) 313-5669

About This Publication

This publication is designed to assist you in the implementation of the Safety Manager Module for use with the Triconex TRICON Version 8 system. Use this document as an informational source, a guide and reference to implementation requirements, and for Safety Manager operational considerations.

All references in this manual to "Safety Manager" or "Safety Manager Module" pertain only for use with the Triconex TRICON Version 8 systems.

Table of Contents

Figures

Tables

Acronyms

AM ..... Application Module
APM ..... Advanced Process Manager Module
APMM ..... Advanced Process Manager Module
BC ..... Bad Control
CL ..... Control Language
CM ..... Computing Module
DEB ..... Data Entry Builder
HM ..... History Module
IEEE ..... Institute of Electrical and Electronics Engineers
LCN ..... Local Control Network
LM ..... Logic Manager
MPES ..... Minimum Physical Event Separation
NIM ..... Network Interface Module
OVD ..... Output Voter Diagnostics
PI ..... Personality Image
PLC ..... Programmable Logic Controller
PMM ..... Process Manager Module
PU ..... Processing Unit
RLL ..... Relay Ladder Logic
SM ..... Safety Manager
SMM ..... Safety Manager Module
SOE ..... Sequence of Events
SSD ..... Sequence Stamp Difference
TDC ..... Total Distributed Control
UCN ..... Universal Control Network
US ..... Universal Station

Parameters

AI ..... Analog Input
AO ..... Analog Output
DC ..... Digital Composite
DI ..... Digital Input
DO ..... Digital Output
OP ..... Output
PV ..... Process Variable
SP ..... Setpoint

References

For TDC 3000^X documentation:

Publication Title	Publication Number	Binder Title	Binder Number
Safety Manager Module Control Functions	SM09-500	Implementation Safety Manager TRICON	TDC 3074
Safety Manager Module Installation Guide	SM20-500	Implementation Safety Manager TRICON	TDC 3074
Safety Manager Module Parameter Reference Dictionary	SM09-540	Implementation Safety Manager TRICON	TDC 3074
Safety Manager Module Configuration Forms	SM88-500	Implementation Safety Manager TRICON	TDC 3074

For TRICON documentation:

Publication Title	Publication Number	Binder Title
TRICON Planning and Installation Guide	9720048-001	TRICON Planning & Installation Guide
TRISTATION MSW User's Manual	9720044-001	TRISTATION MSW User's Manual
Sequence of Events User's Manual	9720042-001	Manuals for Communication Products
Safety Manager Module User's Guide	97200XX-001	Manuals for Communication Products

Section 1 – Introduction

1.1 Implementation Overview

Section summary

This section contains the following topics:

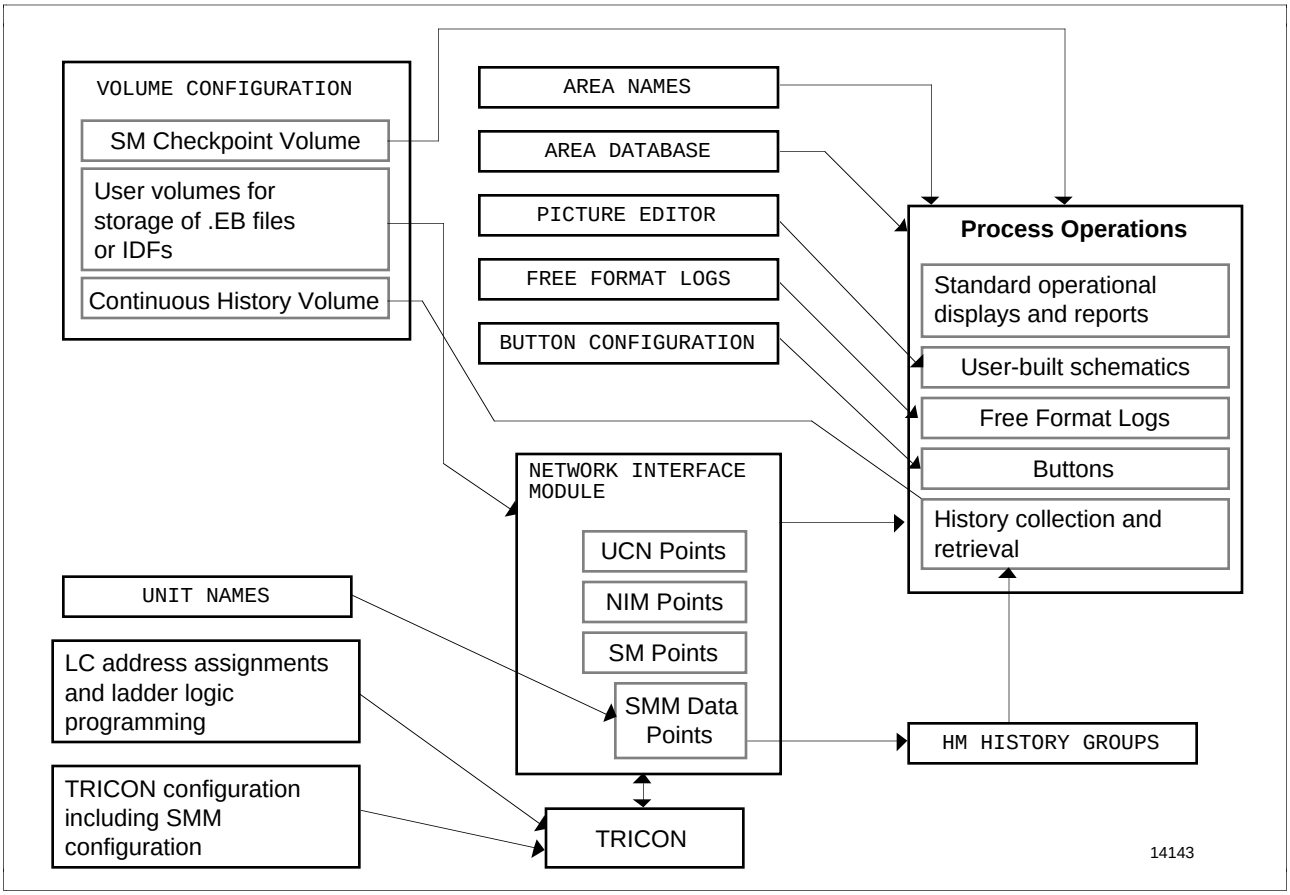
Summary of SM implementation tasks

Though most information in this publication relates to Safety Manager (SM) functions, SM data points and operating considerations, along with other implementation activities must also be completed to make the SM functional.

SM implementation dependencies

Figure 1-1 shows all dependencies that must be completed before the SM can be fully operational. It does not indicate the order of task completion.

Figure 1-1 Safety Manager Implementation Dependencies



Continued on next page

SM implementation tasks

Items outlined in Table 1-1 may be affected by or used to implement an SM.

Table 1-1 Factors Affecting SM Implementation Tasks

Item	Description
Unit Names	The process units are defined for each SM data point.
Area Names	The area name and descriptor are defined for any units with SM points that are assigned to an area.
LCN Nodes	All LCN nodes are defined in this activity. This includes the Network Interface Modules (NIMs) that provide the interface to the Universal Control Network(s) (UCNs) on which the SM resides.
Volume Configuration	The Network Interface Module (NIM) checkpoint volume, &8np, and the CL/PM sequences and &9np, are established in this activity. **ATTENTION** Volume &8np must have adequate storage space to accommodate the SM checkpoint data plus space to accommodate all other devices on all of the Universal Control Networks in this system. Volume &9np must have adequate space to accommodate all CL/PM sequences.
Application Module	Any AM points that are members of a control strategy that includes SM points are built in this activity.
Network Interface Module	UCN points which define to the UCN where an SM resides, and the node-specific points that define the nodes on that UCN, including the NIM and the SM, are built in this activity. Also, SM data points are built in this activity. Connections to the SM points are defined in `tagname.parameter` form. **ATTENTION** Prior to point build, the SM must be configured on the TRICON. TRICON aliases must also be defined.
Picture Editor, Free Format Logs, Button Configuration	Any pictures, logs, and buttons built by these activities can access SM points once the points are built and loaded.
HM History Groups	SM data point values for which continuous history is to be collected are defined in this activity. This is done by assigning them to specific History Module (HM) history groups.
Area Data Base	This activity defines how and where data for data points, including SM data points, are used and displayed in a given process area. The area database is the database loaded into a Universal Station (US)—so that database defines the process area monitored and controlled through the US.
Control Language (CL)	CL/AM and CL/PM programs can access SM parameter values. CL/MC programs cannot access SM parameter values. A Control Language that runs on an SM is not available.
Ladder Logic Programming	This is accomplished through the TRISTATION programming system which is connected to the TRICON's Data Communication Module. TRISTATION provides an interface and software that are installed in a DOS-based IBM or COMPAQ 386/486 personal computer.

1.2 Safety Manager Functional Summary

Safety Manager summary

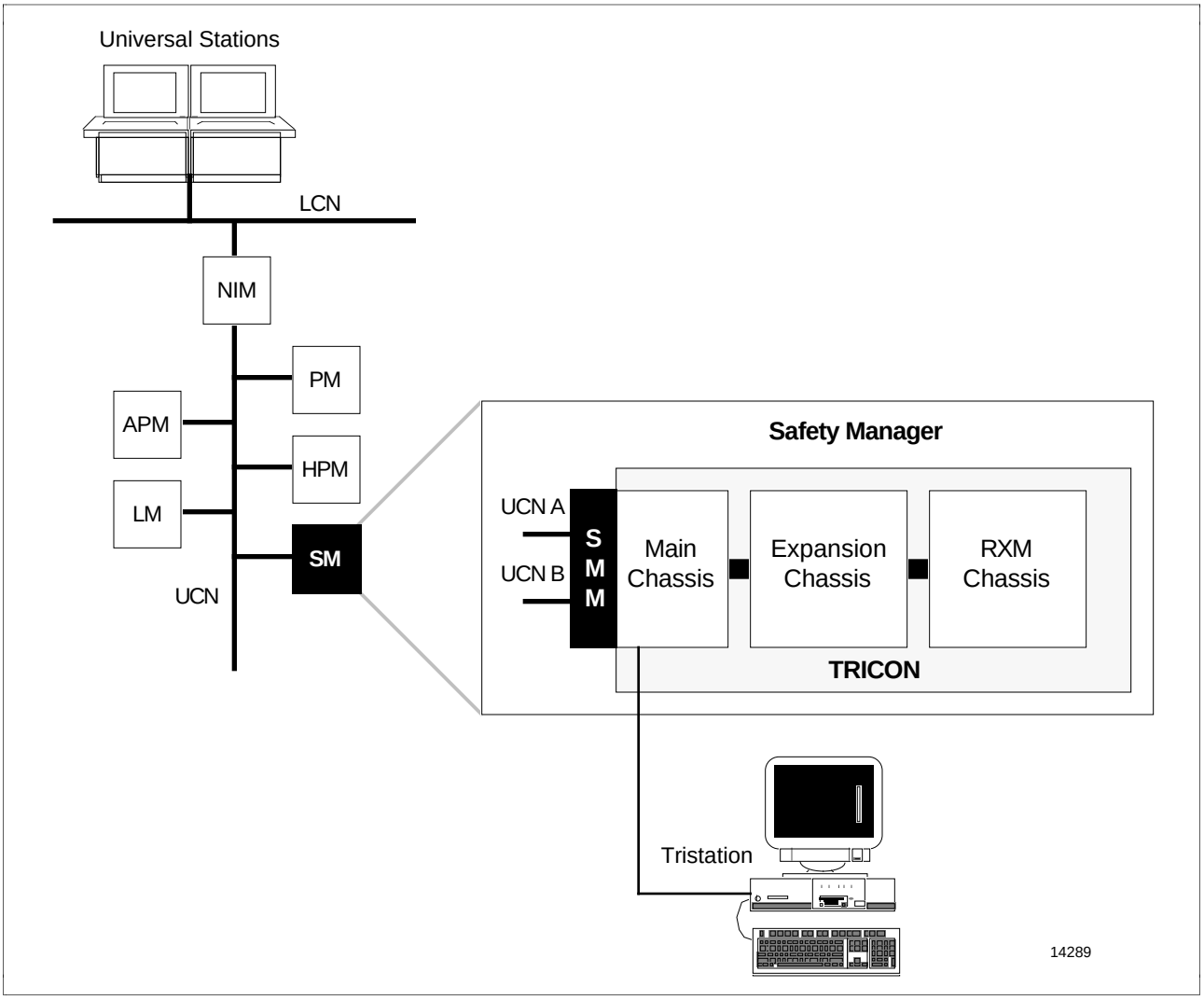
The Safety Manager (SM) provides a Triple Modular Redundant (TMR) fault-tolerant controller for safety and shutdown application on the Universal Control Network (UCN).

The SM consists of a Triconex TRICON controller and a Honeywell Safety Manager Module (SMM). The SMM provides the interface to the UCN.

Safety Manager diagram

Figure 1-2 gives an overview of the Safety Manager connected to the TDC 3000^X network.

Figure 1-2 Safety Manager Relationship to the TDC 3000^X



Continued on next page

1.2 Safety Manager Functional Summary, Continued

Functional overview

The Safety Manager resides as a node on the UCN and consists of these main functional blocks:

- Safety Manager Module
- TRICON controller—including these components:
  - Main Processors,
  - Communication Module,
  - I/O Modules,
  - Power Supply Modules,
  - Chassis, and
  - Fiber-Optic Remote Extender Modules (RXM).

SMM functions

The SMM collects and processes information to and from the TRICON. The SMM converts this data to UCN data types (`tag.parameter`) and performs the following functions:

- engineering unit conversion,
- alarm handling and annunciation,
- diagnostic status reporting, and
- UCN communication functions.

TRICON Main Processor functions

The Triconex TRICON processors read the process inputs and execute the user-written ladder logic program.

Inputs are polled by the Main Processors, voted and processed by the control program and then transmitted to the output modules.

TRISTATION functions

The TRISTATION at the TRICON level of the Safety Manager

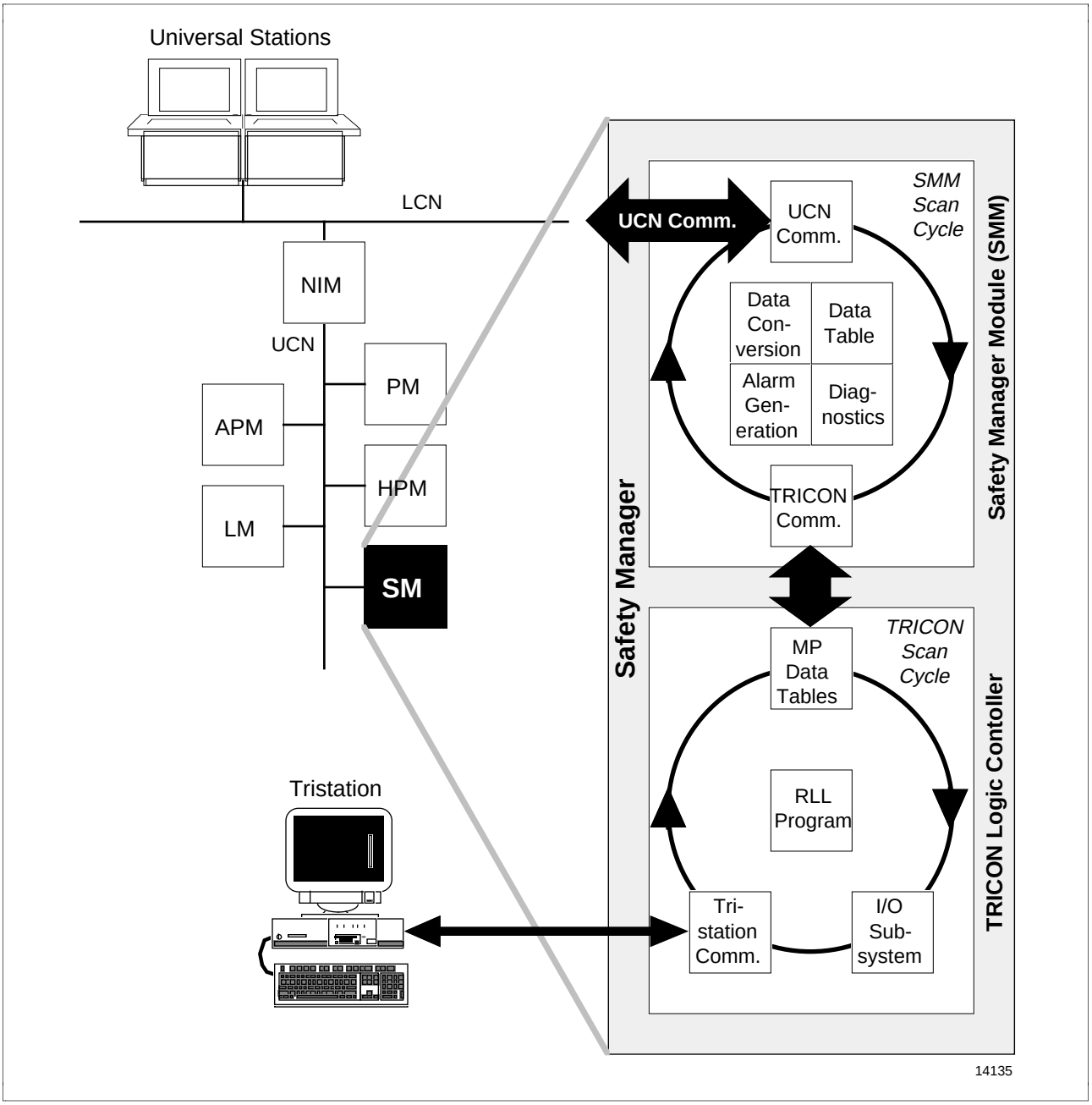
- configures points and parameters,
- creates and loads ladder logic programs,
- displays system status/fault data, and
- forces points for loop check-out and maintenance of field devices.

Continued on next page

Safety Manager functional diagram

Figure 1-3 illustrates the Safety Manager subsystem.

Figure 1-3 Safety Manager Subsystem Conceptual Diagram



1.3 Safety Manager Data Flow

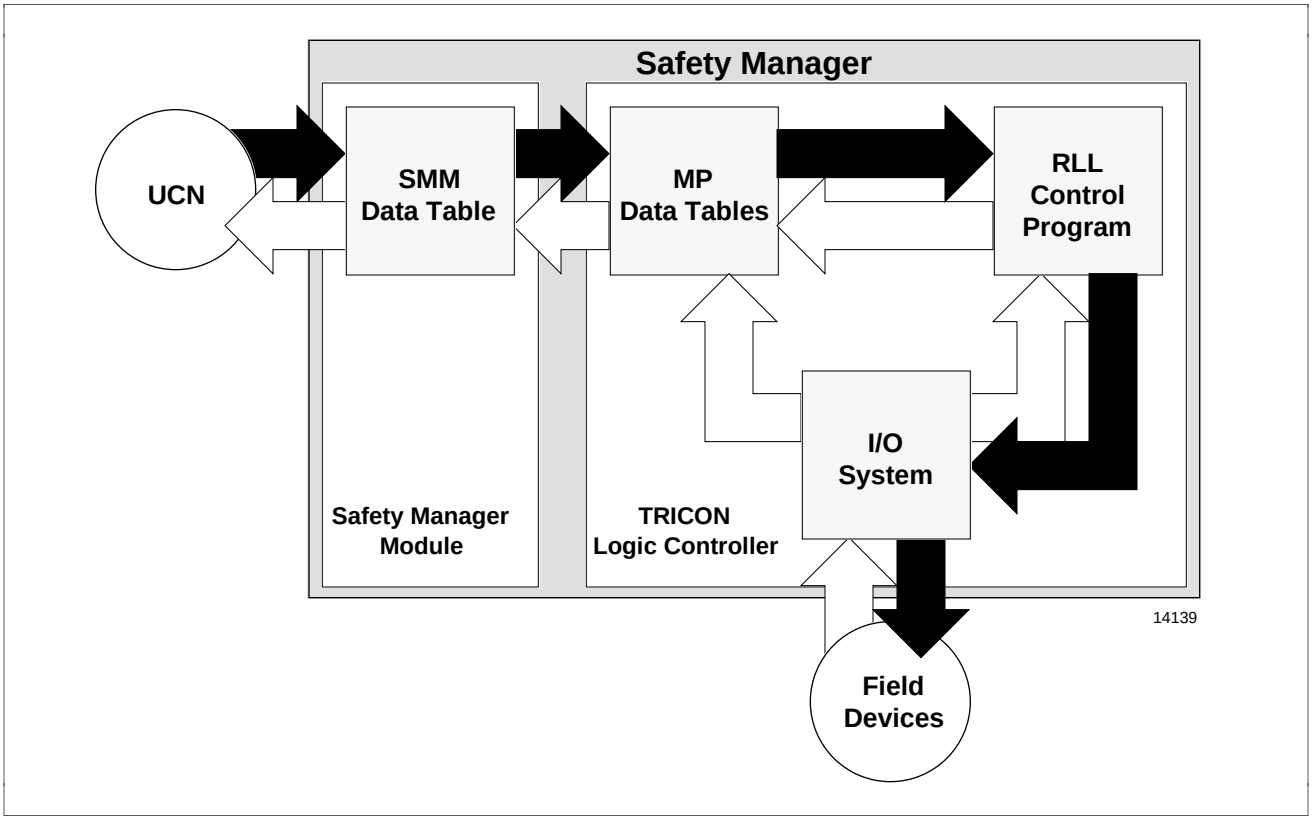
UCN to field and back

As illustrated in Figure 1-4, data being written to, and read from, the I/O system takes two paths within the Safety Manager.

- The UCN output path receives data
  - from the UCN,
  - posts the data in the SMM's Data Table,
  - transfers the data to the MP's Data Tables,
  - processes (tests, modifies) the data in the RLL control program,
  - posts the processed data back to the MP's Data Table, and
  - sends the processed data to the field via the I/O system.
- The UCN input path collects data
  - directly from the field via the I/O system,
  - posts the data in the MP's Data Tables,
  - transfers the processed data to the SMM's Data Table, and
  - places the data on the UCN.

The Relay Ladder Logic control program running in the TRICON is in the path between the SMM output data points and the I/O subsystem. The RLL control program is capable of altering the data output from a Universal Station and the raw input data from the process. It is important to understand what the ladder logic is doing, as it is not possible to view the RLL control program from the US.

Figure 1-4 Data Flow—UCN to Field and Back



Section 2 – SM Operational Considerations

2.1 Safety Manager Operating Modes

Section summary

This section contains the following topics:

Keyswitch function

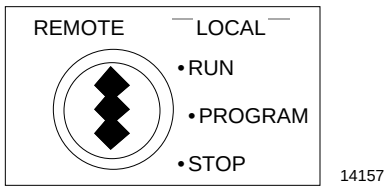
The Safety Manager's operating modes are controlled by a keyswitch on the TRICON main chassis. The four-position keyswitch enables or disables control functions for the entire SM.

The state or position of the keyswitch is readable by the TRICON, TRISTATION and the Universal Station.

Keyswitch mode diagram

Figure 2-1 shows the various positions available for the SM Triconex/TRICON system.

Figure 2-1 SM Triconex/TRICON Keyswitch Positions



Continued on next page

Keyswitch modes

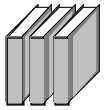
A description of TRICON operating (keyswitch) modes and how they are linked to the SMM is outlined in Table 2-1.

Table 2-1 SMM/TRICON Operating Modes

TRICON Keyswitch Position	Description	SMM
RUN	**Normal operating state.** The main processor executes the previously loaded application program. Attempts to modify program variables from TRISTATION, SMM, or MODBUS masters will be rejected.	IDLE or RUN
PROGRAM	**Programming state.** Allows control of the TRICON system from the TRISTATION software, such as program loading and checkout. If certain conditions are met, attempts to modify program variables from SMM are allowed.	IDLE or RUN
STOP	**Servicing state.** TRICON stops reading field inputs, forces non-retentive digital and analog outputs to 0. It also halts control program scanning. **ATTENTION** The Stop setting is recommended for installation and service of process-related equipment, but it is not required for service of the TRICON.	IDLE
REMOTE	**Alternate operating state.** The main processor executes the previously loaded application program. Attempts to modify program variables from TRISTATION will be rejected, but those from SMM or MODBUS masters are allowed.	IDLE or RUN

ATTENTION The SMM start-up (e.g., ALIVE) and halted (e.g., FAIL) states are possible during any TRICON state. In addition, SMM IDLE and RUN states include softfail forms of IDLE and RUN.

The TRISTATION can halt programs while the keyswitch is in the PROGRAM position. Once this is done, the TRICON will start up automatically when halt is no longer applied. The Safety Manager system will not automatically start, however. It must be commanded to do so.



Refer to Triconex *TRISTATION MSW User's Manual* for further details.

Run mode

The run mode is the Safety Manager's principal operating mode. In this mode, the relay ladder logic program scan operates from the TRICON, executing the program. Attempts to modify program variables from the TRISTATION or the Universal Station will be rejected.

Continued on next page

Program mode

The program mode is where changes to the relay ladder logic control scheme can be made using the TRISTATION. When using the TRISTATION for this purpose, there are several tools (screens) available for altering your control program. These are outlined in Table 2-2.

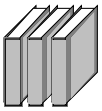
Table 2-2 Program Mode Editing Screens

Editing Screen	Description
File Manager	Provides the tools necessary for managing your program file—including downloading and saving program changes and creating and saving new files.
Ladder Editor	A free-form editor used to develop the logic of your control program. It combines discrete, sequential, control-language elements from the relay ladder language with specially defined expression boxes.
Dictionary Editor	Allows you to manipulate the variables of a control program to • describe program variables with logical names, • define data representation for the variables, • configure variables to represent input and output points on a TRICON, and • search for specific variables and their data definitions.
Module Configuration	Allows you to specify the TRICON hardware configuration for your system. This screen is used to configure the SMM within the TRICON.
Setup Manager	Includes performance of the following functions: • connecting or disconnecting a TRISTATION from the TRICON, • setting the scan rate and calendar of the TRICON, • changing to a different security level, and • changing passwords for the levels that are defined.
Diagnostics	Has the following purposes: • displaying all I/O modules, including the current control program, • providing specific information about faults, and • enabling/disabling and monitoring Output Voter Diagnostics for output modules.
Monitor	Allows you to observe and manipulate the execution of a control program.
Print Manager	Allows you to print any files residing on your computer.

Continued on next page

Program mode, continued

ATTENTION RLL and Alias assignments within the TRICON cannot be modified from the US, LCN, or UCN levels.



For further detail on programming relay ladder logic in the TRICON using the TRISTATION, refer to Triconex's *TRISTATION MSW User's Manual.*

2.2 Address Aliases

Alias address

An alias number is a five digit number that is automatically assigned to a variable in the TRICON that allows nodes on the UCN to reference that variable.

The Alias is a convention of MODBUS, an industry-standard protocol adopted by Triconex for use with its communication modules. Each Alias contains a MODBUS message type and the address of the variable in the TRICON.

Alias ranges, data types, and access rights

Table 2-3 lists the various TRICON alias ranges, data types, and access rights for the Safety Manager Module (SMM).

Table 2-3 TRICON Alias Ranges, Data Types, Areas, and SMM Access Rights

TRICON Alias Range	TRICON Data Type	TRICON Area	SMM Access Rights
1 - 2000	Discrete	Output	Read Only
2001 - 4000*	Discrete	Memory/Output	Read/Write
10001 - 12000*	Discrete	Input	Read Only
12001 - 14000*	Discrete	Memory/Input	Read Only
30001 - 31000	Integer	Input	Read Only
31001 - 31382	Integer	Memory/Input	Read Only
32001 - 32120	Real	Input	Read Only
33001 - 34000	Real	Memory/Input	Read Only
40001 - 40250	Integer	Output	Read Only
40251 - 40632	Integer	Memory/Output	Read/Write
41001 - 42000	Real	Memory/Output	Read/Write

*DISOE limited to these aliases

Linking SMM points to TRICON aliases

There is a one-to-one correlation between a given alias within the TRICON and its corresponding alias configured for an SMM point. SMM output points, however, cannot be mapped to TRICON outputs.

TRICON programming only (i.e., RLL) affects real output control. A write protect flag is configured by the TRISTATION. This flag prevents all write from the US to the TRICON using the SMMs. This limitation is essential to maintaining the integrity of a safety shutdown or critical process controller.

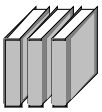
Continued on next page

Assigning alias numbers to elements

You must use the TRISTATION's Dictionary Editor screen to assign aliases to TRICON points. For input and output points, the TRISTATION automatically assigns alias numbers sequentially from the available aliases. These numbers cannot be changed.

If you add a new I/O module to an existing configuration, new alias numbers will be added sequentially from the available numbers. Note that existing alias numbers for other modules will not be disturbed.

For Memory elements, the system displays the first available default alias number from the appropriate range. You can use that number or enter another alias number falling within the specified range. Additionally, you can choose whether the Memory element should be assigned to a Read Only or Read/Write range of MODBUS aliases.



For more information on address aliasing, refer to Triconex's *TRISTATION User's Manual.*

2.3 I/O Subsystem

I/O subsystem

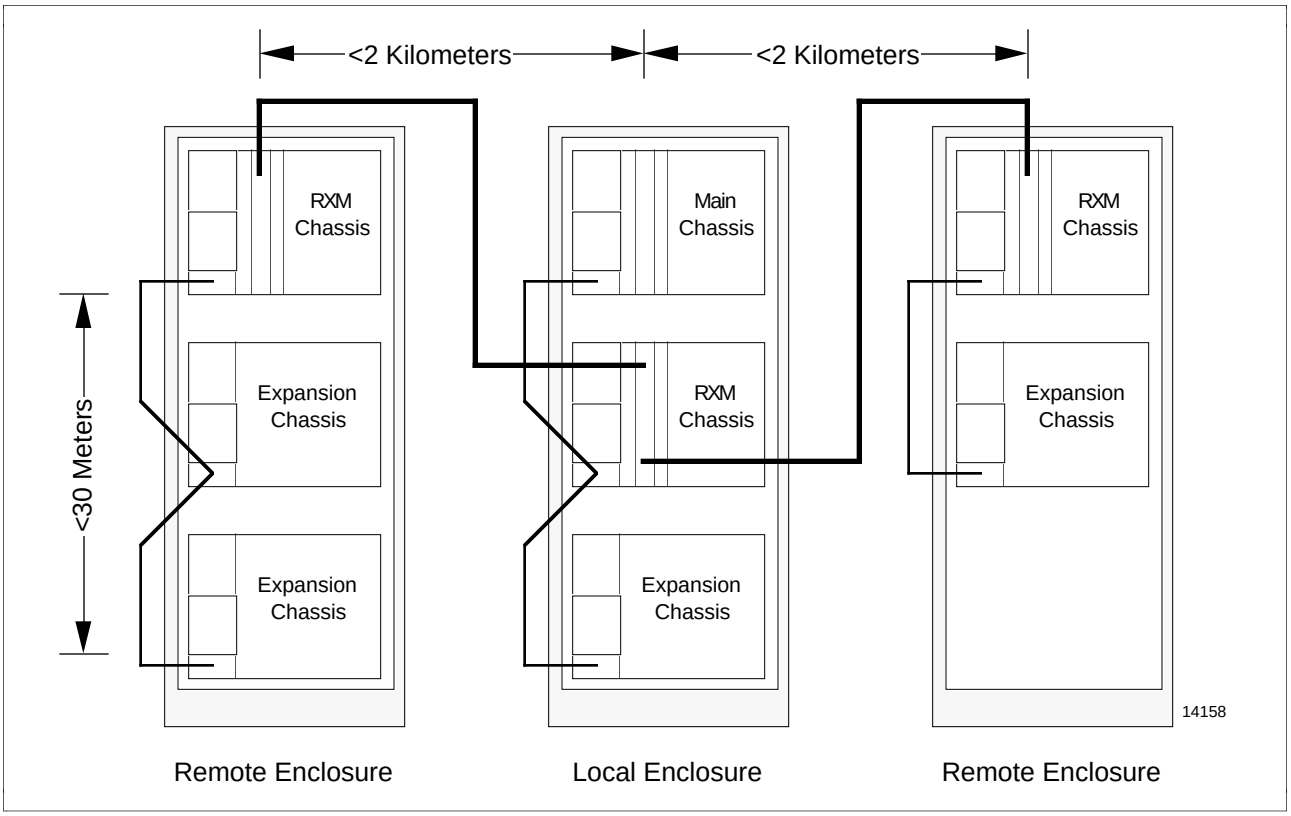
The TRICON's main chassis supports up to four I/O sets and an expansion chassis supports up to five I/O sets. Each I/O set consists of:

- an input or output module,
- an optional hot spare I/O module, and
- a field termination module.

I/O subsystem diagram

Figure 2-2 is an example diagram of an I/O subsystem configuration.

Figure 2-2 Local and Remote I/O Subsystem Configuration Example



I/O types supported

The Safety Manager, using the TRICON, supports digital and analog input and output points, as well as thermocouple inputs. Internal and external termination of these points is offered as well.

Continued on next page

I/O characteristics

Table 2-4 describes the associated I/O characteristics with the various module types.

Table 2-4 I/O Characteristics for the Various Module Types

Field Inputs	Field Outputs	MODBUS	802.3
• 24-115 Vac/Vdc • Analog (0-10 Vdc) • Pulse • Isolated Thermocouple • Non-isolated Thermocouple	• 48-115 Vac • 24-120 Vdc • Analog (4-20 mA) • Relay	• EICM • HIM	• DCM • NCM

I/O capabilities

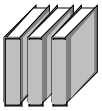
The SM Triconex/TRICON supports up to 74 I/O modules (analog, digital, and communication). In addition, the TRICON provides integral support for remote I/O modules located up to 2 kilometers (1.2 miles) from the main chassis.

Intelligent I/O

Each I/O module has input and output microprocessors. Input microprocessors filter/debounce the inputs and diagnose hardware faults on the module.

Output module microprocessors

- supply information for the voting of output data,
- check “loopback” data from the output terminal for final validation of the output state, and
- diagnose field-wiring problems.



For more detailed information on I/O architecture, functions, and capabilities, refer to Triconex’s *TRICON Planning and Installation Guide.*

2.4 Sequential Events Recorder (SER)

SER summary

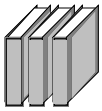
The Sequential Events Recorder (SER) is an application package for the TRICON which records selected events in real time. It provides a tool to determine the cause of a trip or shutdown.

SER allows you to create a database of TRICON variables for which you wish to observe. It also gives you the ability to specify parameters for collecting this data.

SER database using the TRISTATION

Before SER can be set up for data collection, TRISTATION must be used to prepare the SER database. The following items must be completed to use the SER:

- A trip value must be defined in the control program.
- All variables for which the SER will collect data must have Alias numbers assigned to them.
- A .DPT file of Aliased variables must be created with the Dictionary Editor.



For more information regarding the SER, refer to Triconex's *TRICON Technical Product Guide.*

ATTENTION

ATTENTION—SER configuration has no impact on SMM Sequence of Events operation.

CAUTION

CAUTION—TRICON clock synchronization operations from the SER tool will be overridden by SMM time synchronization.

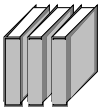
2.5 Sequence of Events (SOE)

SOE summary

During each program scan, the TRICON's Main Processor (MP) examines designated discrete input variables for a change of state (an event). When the TRICON detects an event, it saves the time the event occurred.* SMM digital input (DI) points configured for SOE will then collect these TRICON timestamps for event processing.

*Time stamps applied by the TRICON are on a "per scan" basis.

Up to two logical SMM slots may be configured for SMMs in the TRICON. Two TRICON Main Processor SOE memory blocks are provided, one for each SMM logical slot. Each SMM pair (logical slot) must be configured by the TRISTATION to use one of these blocks.



See the Triconex *SMM User's Manual*, P/N 97200XX-001, *Installing the SMM* for more details.

SM sequence of events configuration summary

SOE within SM involves user configuration of the TRICON and the SMM for

- transparent time synchronization,
- timestamping and event distribution processes, and
- journaling and display of detected events.

Main Processor and SOE

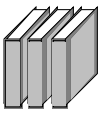
The MP compares the current state of each event variable with its state during the previous scan. If the states are different, the MP records

- the scan's date and time,
- the variable's alias, and
- the variable's current state.

Main Processor memory requirements

MP memory requirements for SOE are dependent on

- the size of your control program,
- the number of points you have configured, and
- the number and size of the SOE blocks you have defined.



Refer to Triconex's *TRICON Planning and Installation Guide.*

Continued on next page

Time synchronization

Time synchronization is transparent to the user and is characterized as such:

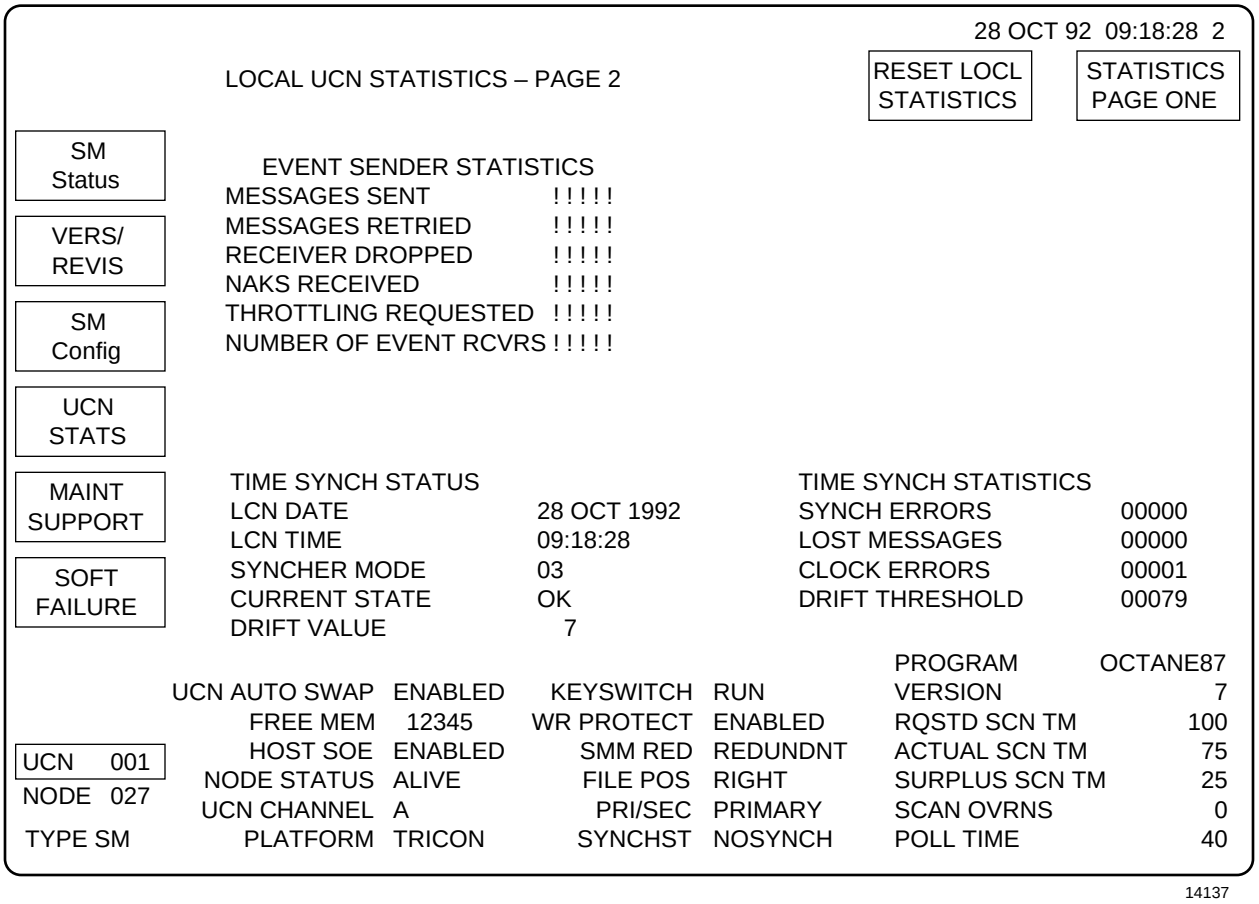
- The NIM provides time synchronization for all nodes on the UCN.
- The SMM synchronizes the clock on the TRICON Main Processors to LCN time—having a clock resolution of 1 millisecond.
- The SM Time Sync will override any attempt by the user to set TRICON time using the TRISTATION Sequence Events Recorder (SER).

ATTENTION Time synchronization must be configured by the TRISTATION. The "Adjust MP Clock" must be set to Yes in the SMM Configuration Menu to enable TRICON time synchronization.

Time Sync diagram

Figure 2-3 shows a US Diagnostic display summarizing Time Sync parameters.

Figure 2-3 Diagnostic Display UCN Statistics—Time Sync Parameters



Continued on next page

2.5 Sequence of Events (SOE), Continued

Comparing events between TRICONs

The NIM and TRICON have time synchronization features which keep time within all the TRICONs within ±3 ms.

The same timestamps of the *same* event recorded by two TRICONs could be off by as much as ±1 scan time of the TRICON with the longer scan ±3 ms.

Timestamping within the TRICON

Timestamps within the TRICON are characterized by the following:

- Timestamps are based on TRICON time measured and voted upon (middle value) following the refresh of the Input Status.
- All detected events within a given TRICON scan will have a timestamp of the same value of time.
- For each TRICON User Program Scan, each MP will monitor all variables listed in the SMM's SOE Block, and timestamp and buffer any detected changes-of-state.
- The SMM will collect the timestamped events using function calls to the TRICON interface.

DI SOE timestamping

DI SOE timestamping is designed to synchronize the SM to the LCN time provided through the NIM, for consistent and comparable timestamping of DI events throughout the TDC 3000^X system.

Timestamping for the SM is the responsibility of the TRICON's Main Processors. The TRICON collects any DI events once per User Program Scan and uses the same clock time to timestamp all events within that scan.

Non-DI SOE event/ alarm timestamping

The SMM will assume responsibility for the timestamping of non-DI SOE alarms and events. Displayed SMM timestamp resolution will be to 1 ms.

SOE resolution

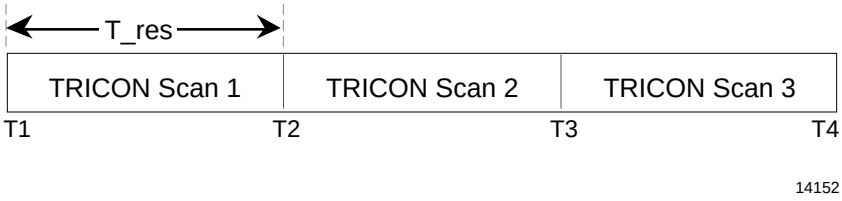
SOE resolution (T_res) is equivalent to the TRICON User Program Scan Time. This scan time is user configurable, but must equal or exceed actual TRICON control program scan time.

Continued on next page

SOE resolution diagram

Figure 2-4 illustrates SOE resolution (T_res) for the TRICON.

Figure 2-4 SOE Resolution



Sequence stamp difference

Sequence Stamp Difference (SSD) is also dependent upon the configurable TRICON User Program Scan Time. It is an integer multiple of the SOE resolution (T_res). It is the smallest difference in timestamps between two DI events that guarantee they occurred in the sequence indicated by their timestamps.

Skew

Skew (T_skew) is the sum of all factors which contribute to different timestamps being applied to the same physical event if wired into different places in the system. The components of skew are the sum of

- SM clock drift,
- SM clock synchronization error,
- DI filtering,
- DI propagation delay, and
- DI scan sequence.

Time delays

Since the DI events are timestamped in the TRICON Main Processors, the maximum difference in delay from two real field events to the reflection of those events in the Main Processor input table, must be considered.

Differences in these delays between two events could cause them to enter the input table on different scans and in a different order than they actually occurred. Table 2-5 gives an example. Figure 2-5 illustrates this occurrence.

Continued on next page

Example of time delay event occurrence

Table 2-5 outlines event occurrence that could possibly lead to the timestamp misrepresentation.

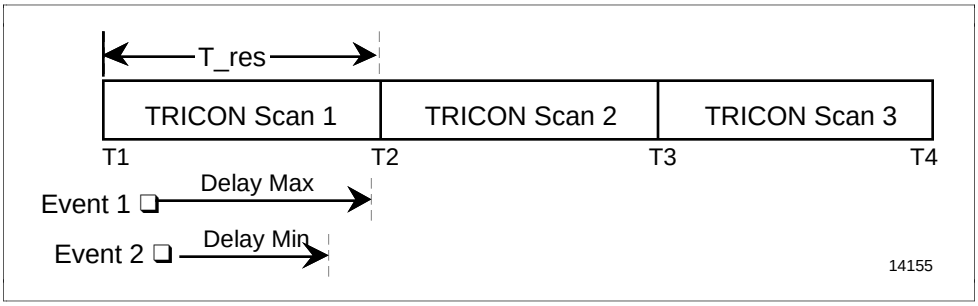
Table 2-5 Event Misrepresentation

Step	Action
1	Event 1 occurs before Event 2 in the field.
2	Event 2 experiences minimum delay and is reflected in the Main Processor Input Table at T2 for scan 2.
3	Event 1 experiences maximum delay — making it too late to be reflected in the Input Table at T2.
4	Event 1 is instead reflected in the Input Table at T3 for scan 3.
5	Event 1 is timestamped with T3 whereas Event 2 is timestamped with T2.

Time delay diagram

Figure 2-5 illustrates an inaccurate timestamp caused by a time delay.

Figure 2-5 Inaccurate Timestamp Due to Time Delays



Correcting time event misrepresentation

The actual SSD is T3–T2, equal to 1xT_res. However, in the previous example, the timestamps do not indicate the correct chronological sequence of events. Therefore, an SSD of 1xT_res is insufficient to guarantee correct sequence.

The SSD for the Safety Manager is therefore at least 2xT_res or 2 TRICON User Program Scan Times (minimum of 100 milliseconds). Unless the difference in Delay Max and Delay Min values are greater than T_res, an SSD of 2xT_res should guarantee correct event sequence as indicated by the timestamps.

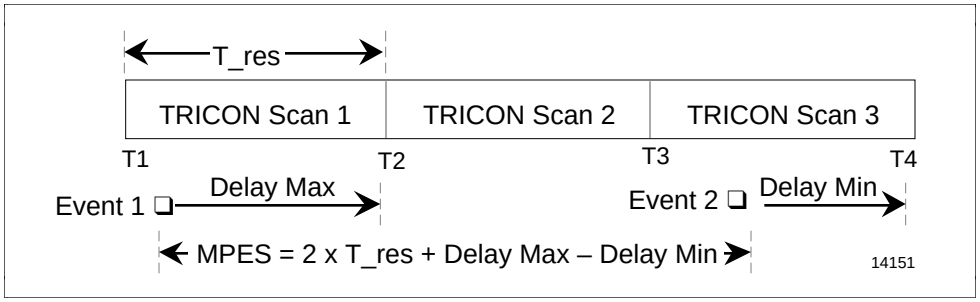
ATTENTION A thorough analysis of the I/O delays (especially for remote serial I/O link) could reveal that the SSD is more than 2x the TRICON User Program Scan Time for some cases. This can happen if the difference between maximum and minimum real DI event to input table delay is greater than T_res.

Continued on next page

Minimum physical event separation

Minimum Physical Event Separation (MPES) is the minimum amount of time which must separate two physical DI events to guarantee they receive timestamps that indicate the correct chronological order of events. This is the sum of SSD and all T_skew. Figure 2-6 illustrates MPES.

Figure 2-6 Minimum Physical Event Separation



ATTENTION Skew for the Safety Manager must be determined before a detailed analysis of MPES can be completed.

SOE event recovery

Event Recovery of timestamped events is characterized by the following:

- Occurs only during SMM or NIM failover/switchover.
- No operator intervention is required.
- The SM will buffer timestamped events for at least 20 seconds.
- SOE Event Recovery will restart a collection from t-20 seconds.
- In failover situations, Event Recovery will involve a reread of events that are equal to or less than 20 seconds of age.
- During buffer overflow situations (no available buffer space and no events older than 20 seconds), the SM will drop new events.

ATTENTION There is no SOE Event Recovery at SMM startup (IDLE-to-RUN transition). Instead, events timestamped within the TRICON (for the SMM) will be given a timestamp of zero.

SOE event recovery cut-off point

SOE Event Recovery ends when

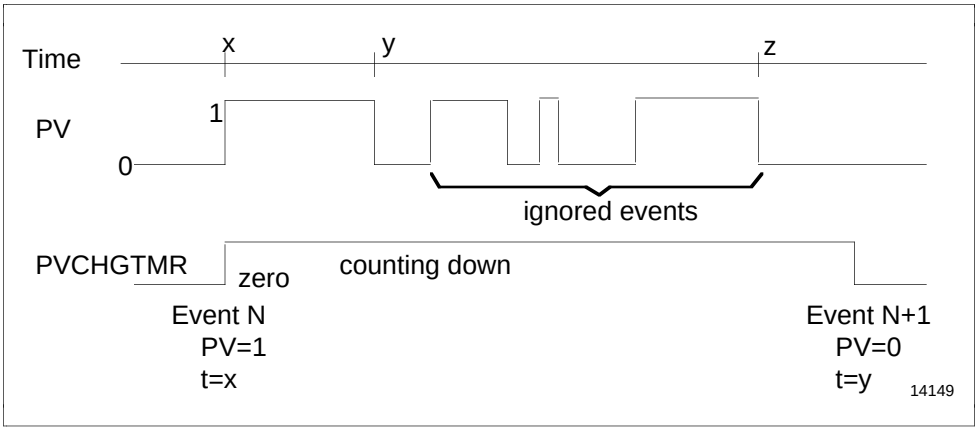
- event timestamps exceed the LCN time at start of recovery and
- the TRICON SOE Event Buffer is emptied.

Continued on next page

Throttled event collection

SMM will filter event bursts through the use of a PV Change Delay function. This function is similar to that available for alarming using the DLYTIME parameter. PVCHGDLY (preset) and PVCHGTMR (timer) are the supporting parameters. Figure 2-7 illustrates how unwanted changes in events are ignored.

Figure 2-7 Throttled Event Collection



Event recovery and flushing

Flushing an SMM database from Primary to Secondary will have the following effect on event recovery:

- Point databases and active delay timers will be flushed to the Secondary.
- Although SOE event data is not flushed, it is maintained in a way such that it will not be lost.

Event distribution

SOE Event Distribution is characterized by the following:

- Similar to the APM, a separate Event Distribution process will allow alarm events to be distributed at a higher priority than other events on the UCN.
- SMM will distribute timestamped events per established UCN procedures.
- Total local alarm and event output is limited to 512 over any 10 second period.

Continued on next page

Journals and listings

Displayed timestamp resolution will be to 1 ms, with Sequence Stamp Differences equivalent to TRICON Scan Time.

SOE configuration

To use SOE, you must

- define the SOE block for each SMM (or redundant pair),
- start the collection of data in the SOE blocks within the ladder program,
- configure the selected DI points to be collected for SOE on the TDC 3000^{X}, and
- assure Time Sync feature on the associated NIM is enabled.

SOE block

An SOE block is a data structure that resides in the MP's memory. A block contains the

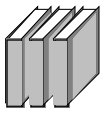
- block type,
- buffer size, and
- list of the variables included in the block.

There are 16 SOE blocks available. Blocks 15 and 16 are External blocks for use with the SMM only. You can configure the remaining 14 SOE blocks using any combination of the other block types.

SOE block types available

There are four block types. The difference between the four block types is the way in which the MP handles a buffer-full condition. Descriptions of the four types are listed below.

- Historical—the MP overwrites the oldest event entries.
- First Out—the MP changes the block's status from collecting to stopped and discards new event entries.
- External—the MP discards new event entries.
- External (used with the SMM only)—the SMM (vs TRICON) handles recovery by not acknowledging events until they are 20 seconds old.



For more information on SOE block configuration, refer to Triconex's *TRISTATION MSW User's Manual* or Triconex's *SMM User's Guide.*

2.6 Saving and Restoring Safety Manager Data

Restoring and saving data summary

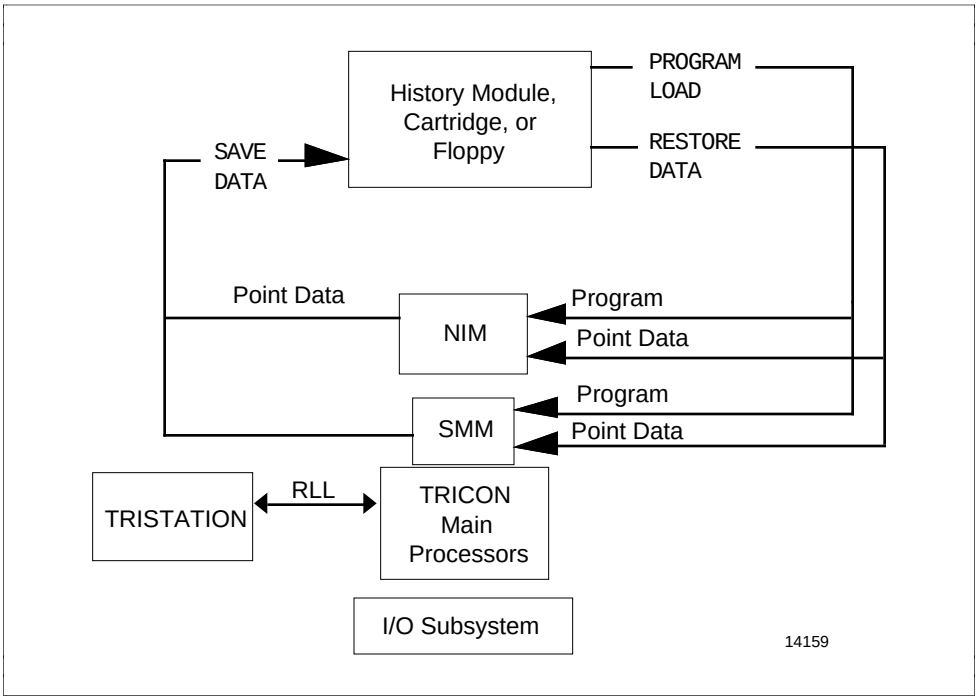
Checkpoint saving/restoring and saving/restoring relay ladder logic (RLL) are separate operations. RLL programs are saved and restored in the SM using the TRISTATION. Checkpoint saving and restoring is done at the US.

Refer to Triconex's *TRISTATION MSW User's Manual.*

Saving/restoring data flow

Figure 2-8 shows the saving and restoring data flow for the Safety Manager.

Figure 2-8 SM Saving and Restoring Data Flow

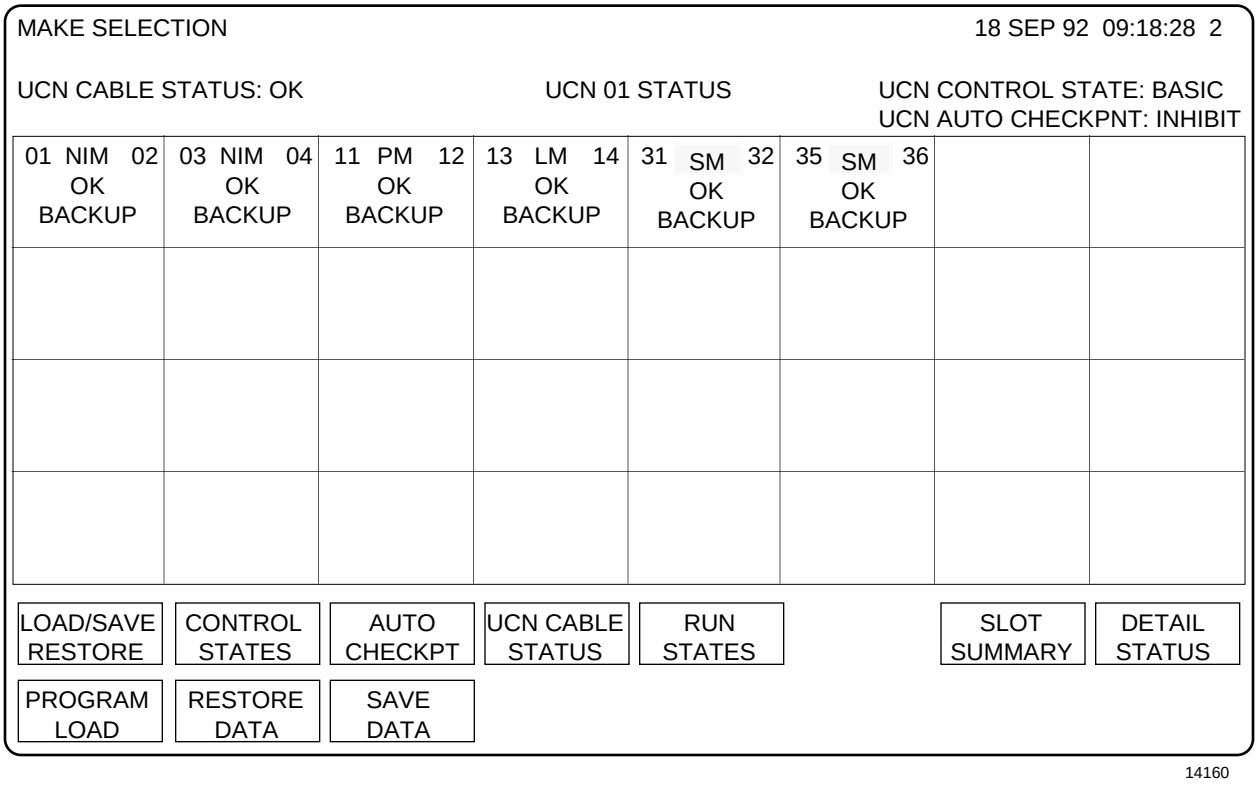


Continued on next page

Saving and restoring data using the US Status display

The three bottom targets of the UCN Cable Status display, shown in Figure 2-9, save and restore the NIM and Safety Manager data points.

Figure 2-9 US Status Display - Data Save and Restore



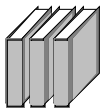
Continued on next page

Function of save and restore targets

Table 2-6 outlines the functions of the US Status display save/restore targets.

Table 2-6 Save and Restore Command Functions

Command	Description
PROGRAM LOAD	Loads the NIM and SMM software personality image from the &UCN volume on an HM, or from a cartridge or floppy, to the NIM and selected SMM(s) in the selected Safety Manager(s).
RESTORE DATA	Restores point data stored in the &8np checkpoint volume on an HM, or from a cartridge or floppy, to the NIM and the SMM(s) in the selected Safety Manager(s).
SAVE DATA	Saves point data in the NIM and SMM (s) in the selected Safety Manager(s) into the &8np checkpoint volume on an HM, or onto a cartridge or floppy. This target requests a “demand” checkpoint. Automatic checkpointing may also save this data at the established automatic checkpoint interval for this system.

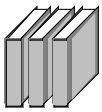


For more information on checkpointing, refer to Section 21 of the *Engineer’s Reference Manual* in the Implementation/Startup and Reconfiguration-2 binder.

2.7 Battery Backup Considerations

Power supply battery backup

The Safety Manager power supply system is backed up with a battery that is designed to maintain data and programs for approximately six months.



To replace the power module battery located on the TRICON, refer to Triconex's *TRICON Planning and Installation Guide.*

SMM battery backup

The SMM contains a lithium battery that serves to maintain memory content in the absence of primary power. The SMM's battery backs up its internal memory.

The battery may be protected from discharge by using a wafer. You can also just unplug the SMM from the chassis to prevent discharge.

Like all TRICON modules, you can install an SMM into a running TRICON system with power on (hot insertion). The battery only discharges when the SMM is installed in a TRICON chassis and the chassis is not powered. If you remove the SMM from the chassis, the SMM's memory is lost and the battery does not discharge.

ATTENTION While the SMM battery provides reliable backup of the memories in the absence of primary power, it does not absolutely assure the retention of data in the memories.

Battery failure causes a SOFTFAIL status to appear at the US.

Section 3 – Redundant Safety Managers

3.1 Redundancy Overview

Section summary

This section contains the following topics:

Overview

The Safety Manager redundancy scheme is made up of two components.

- TRICON—Triple Modular Redundancy (TMR) configuration.
- SMM—hot spare module within the same logical slot.

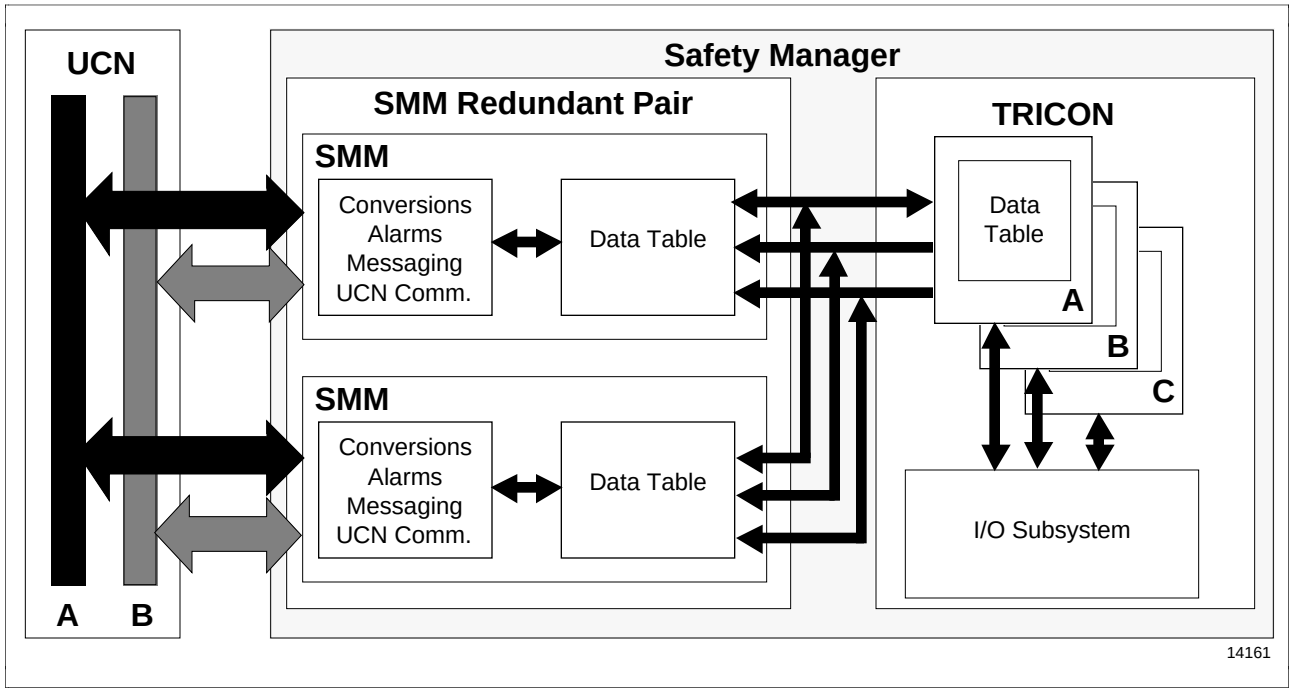
This subsection will focus primarily on the Safety Manager SMM redundancy. For TRICON TMR redundancy, refer to Triconex's *TRICON Planning and Installation Guide.*

ATTENTION SMM redundancy does not interfere with TRICON redundancy. In addition, failures within the TRICON processors or I/O will not impact SMM redundancy status.

SMM /TRICON redundancy scheme

Figure 3-1 shows the redundant architecture of the SMM and TRICON controller.

Figure 3-1 Redundant Safety Manager System Connected to the UCN and TRICON

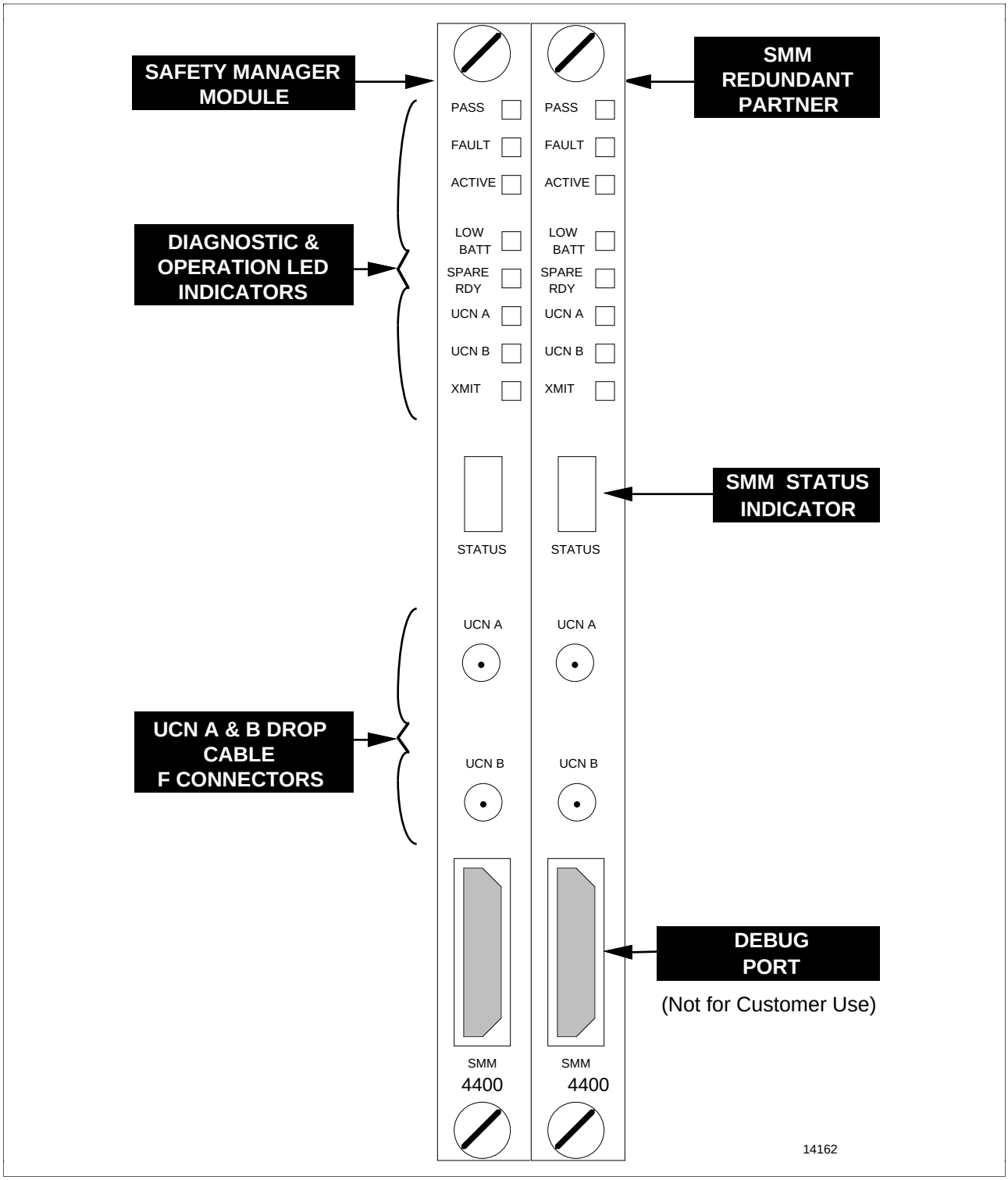


Continued on next page

Safety Manager redundancy diagram

Figure 3-2 shows the front panel of a redundant Safety Manger system.

Figure 3-2 Redundant Safety Manager



Continued on next page

SMM front panel indications

PASS, FAULT, and ACTIVE indicators, as seen in Figure 3-2, operate per TRICON Communication Module procedures. Table 3-1 gives an overview of the description of each.

Table 3-1 SMM Front Panel Indications

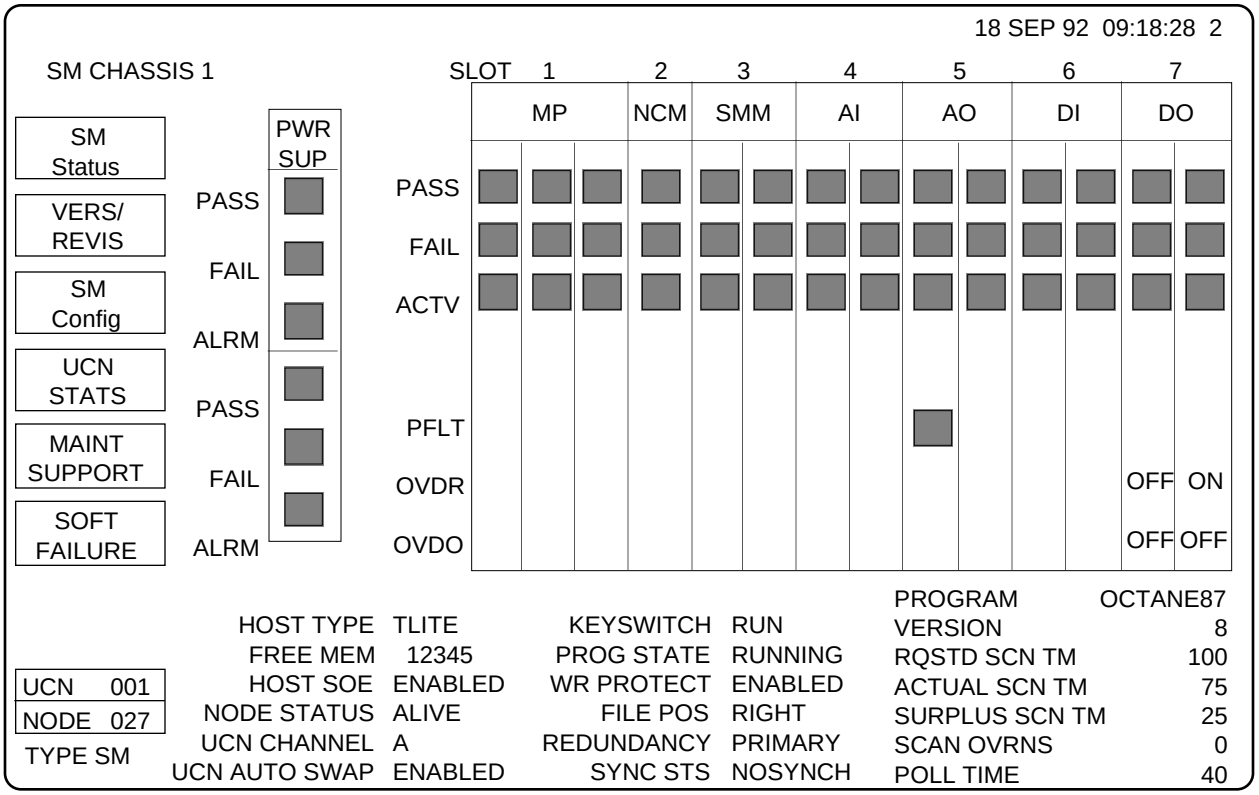
PASS*	FAULT*	ACTIVE*	Description and Action
1	**0**	**1**	Module is operating properly as a non-redundant or Primary SMM.
1	**0**	**0**	Module is operating as a Secondary (hot spare) SMM. Refer to the Operator Station Diagnostic Displays or the Alphanumeric Status Indicator Display on the SMM for specific state information.
0	**1**	**1**	Module is active, but has detected a fault.
0	**1**	**0**	Module is not active. Module is initializing or has detected a fault.
1 **0**	**1** **0**	**X** **X**	The indicators/signal circuitry are malfunctioning.

*Where 1 indicates on; 0 indications off; and X indicates not available.

SMM redundancy configuration

Figure 3-3 shows a US Display of a chassis configured for a redundant SM.

Figure 3-3 US Display—Redundant Safety Manager Configuration



Continued on next page

SMM redundancy functional summary

The SMM offers functionally redundant communications modules with redundant ports and paths operating continuously. SMM redundancy consist of two major tasks:

- self diagnostics and switchover control, and
- SMM database synchronization.

SMM and TRICON redundancy interfacing

The SMM will monitor its three links to the Main Processors. A fault in this interface will trigger the SMMs to choose the best of two TRICON interface situations. The failure of a link to a TRICON MP will not necessarily dictate a failover. Instead, the SMMs will attempt to isolate the failure and maintain the most effective interface.

Redundant SMMs channel switchover requests through the UCN, Private Link, and the Comm Bus to provide security against failure. When a failure does occur, various subsystems will either flag the Diagnostic Manager or kill the module entirely when a fault situation happens.

ATTENTION Existing TRICON module installation guidelines, as they pertain to redundant communication cards, must also be followed with redundant SMMs. SMM configuration is done using the TRISTATION.

SMM failover

Failover involves the fault-initiated shutdown of an SMM Primary followed by the Secondary's assumption of the Primary State. Failovers are the result of an SMM or SMM interface fault. SMM redundancy failover occurs in five seconds or less—when measured from primary failure to where the (new) primary SMM completes a priming scan.

The faults that can cause a failover to the SMM hot spare include the following:

- The on-line SMM stops communicating with the Main Processors.
- The hot spare SMM is receiving information from the UCN, but the on-line SMM is not.
- The on-line SMM encounters an internal failure.

SMM switchover

SMM switchovers result from an Operator Station command. For operator-requested switchovers, the SMM will complete Primary/Secondary switchover and Point Processing priming within two Point Processor Scan Times (normally two seconds). An additional 0.5 seconds (two seconds maximum) will be required for Secondary resynchronization.

Continued on next page

SMM switchover procedure

To began operator-initiated switchover, you must follow the procedure outlined in Table 3-2. Figure 3-4 shows this procedure graphically.

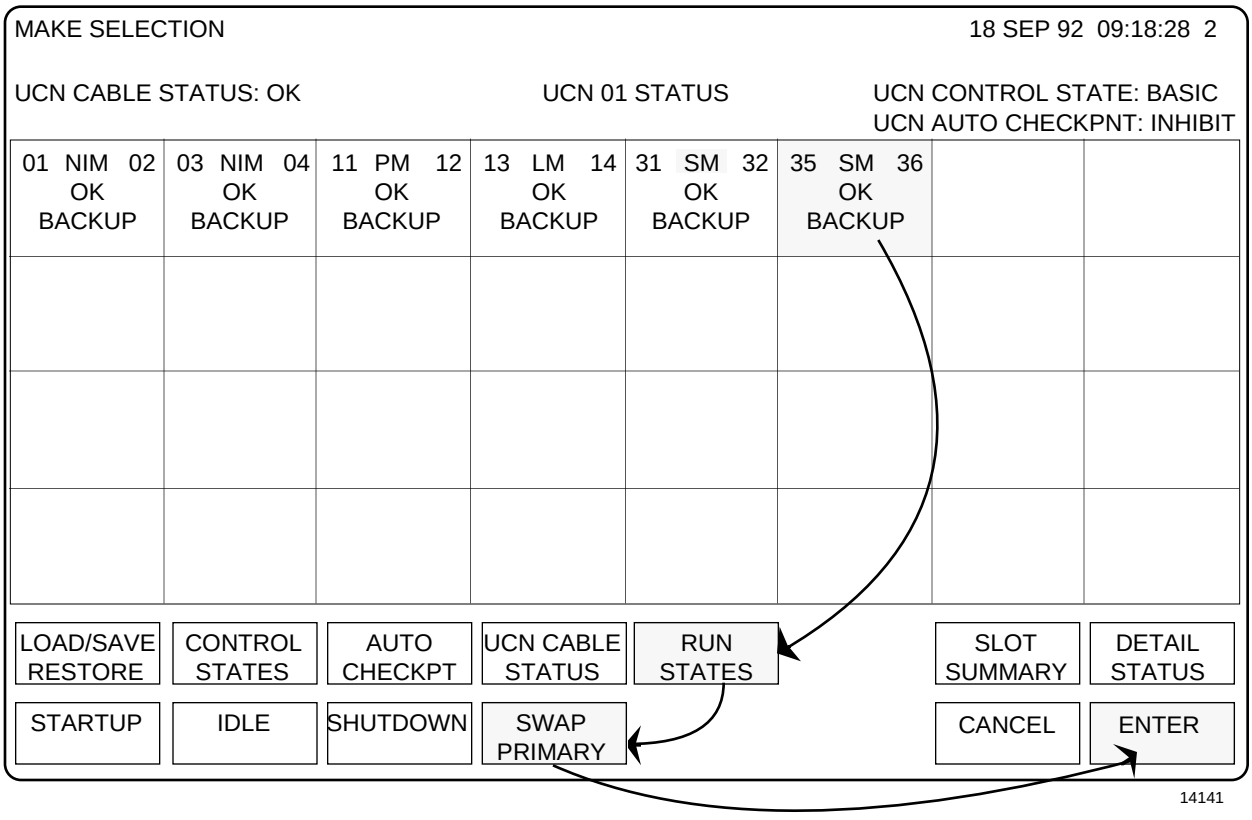
Table 3-2 SMM Switchover Procedure

Step	Action
1	Select target node from US UCN CABLE STATUS display.
2	Select “RUN STATES” target.
3	Select “SWAP PRIMARY” target.
4	Select “ENTER” target.

US UCN status display for SMM switchover

Figure 3-4 shows the US UCN Status display used for operator-initiated SMM switchover.

Figure 3-4 US UCN Status Display for SMM Switchover



3.2 SMM Database Synchronization

SMM database synchronization

The following are characteristics of SMM database synchronization:

- The SMM Primary will not automatically failover to an unsynced Secondary unless that Primary is unable to communicate over the UCN.
- Following operator requested switchovers, SMM database synchronization will occur in five seconds or less for a maximum 150 Kbyte database.
- If the Secondary is unsynced, the SMM will reject operator-initiated switchover requests.

SMM flushing

Flushing is the act of copying database changes between redundant pairs and is characterized by the following:

- Flush operations occur in under 0.125 seconds.
- There is no need to synchronize or flush any TRICON data.
- Parameter writes are flushed to the Secondary prior to UCN acknowledgment.
- Done over the Private Link or UCN.

Primary/secondary SMM UCN time sync

Both SMM Primary and Secondary will participate in UCN Time Sync. However, TRICON time sync is the responsibility of the SMM Primary. Upon SMM failover/switchover:

- The new SMM Primary will initiate Event Recovery and issue a request to the TRICON to retransmit timestamped events which were buffered over the last 20 seconds.
- The new SMM Primary will assume responsibility for TRICON time sync.

Private Link

A PM-like 5 Mbs Private Link will interconnect the SMMs across which database sync and flush and status and control transfers will occur.

There is no need for user configuration of the Private Link. An SMM will use its UCN Nodal Address on the Private Link and will expect a matching Nodal Address (±1) to be used by the SMM connected to that Private Link.

Continued on next page

Private Link failure

Should the Private Link path fail, it will be treated as a softfail. This will allow the SMMs to maintain a view of the process.

The SMMs will resolve Primary/Secondary status based upon UCN communications. The SMM will use the UCN as a backup path for database sync and flush operations. This will be done to maintain redundancy and allow the installation of a replacement SMM.

SMM redundant communication paths

SMM redundant communication paths are characterized by the following:

- Functionally redundant communication modules with redundant ports and paths operate on a continual basis.
- SMM initiates the switchover of SMMs at the Comm Bus level by issuing requests to the TRICON to set the SMM active or inactive.
- SMM uses the UCN to exchange data between redundant SMMs.
- SMM uses an intraslot (Primary to/from Secondary) messaging service provided by the TRICON. This additional communications path assists the SMMs in diagnosing Private Link, UCN, Comm Link, or partner SMM problems.

UCN-specific SMM redundancy

UCN-specific SMM redundancy is characterized by the following:

- On-line and spare SMMs have unique addresses, allowing both to participate in UCN communications.
- Only the primary SMM in a pair can send point information on the UCN at any given time.
- The SMM uses the UCN to also exchange RDR (status) records between redundant SMMs.
- From the UCN's perspective, SM redundancy emulates that of other UCN nodes. This includes redundant cable interfaces, cable handling algorithms, redundant nodes, fixed UCN Shadow Addressing, reconfigurable Primary/Secondary UCN Nodal Addressing, UCN Status Display handling and redundancy status parameters.

ATTENTION If retries result in continued use of incorrect partner addressing, an SMM that is in a start-up sequence (vs. an Idle or Run state) will crash, having assumed that it could be corrupting the UCN.

3.3 Other Redundancy Considerations

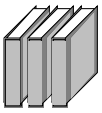
UCN addressing

The UCN address is configured by the TRISTATION and loaded with the control program into the TRICON Main Processors. TRISTATION only allows odd UCN addresses to be configured.

In the ALIVE state, the SMM will display the odd address in left slot or even address in right slot.

In the IDLE/RUN states, the primary assumes the odd address (where points are built) and the secondary assumes the even (backup) address.

When the SMM is installed, the TRICON Main Processors load the UCN address, along with the SOE block number, Write protect flag, Time synchronization flag, and UCN test mode flag into the SMM.



See the Triconex *SMM User's Manual*, P/N 97200XX-001, *Installing the SMM* for configuration details.

Preference

Preference toward one of the SMMs enables the redundant pair to better resolve contention situations. Preference is based on right/left file position, the left is preferred (a TRICON convention).

Hard failure

Hard failure situations will result in SMM shutdown (to the FAIL state or total reset). Hard failure situations include component, program, or database failures which may or may not interfere with MP operation, but are considered detrimental to either the TRICON, the partner SMM, or the UCN.

ATTENTION The absence of communications will serve to signal the partner SMM of the failure situation.

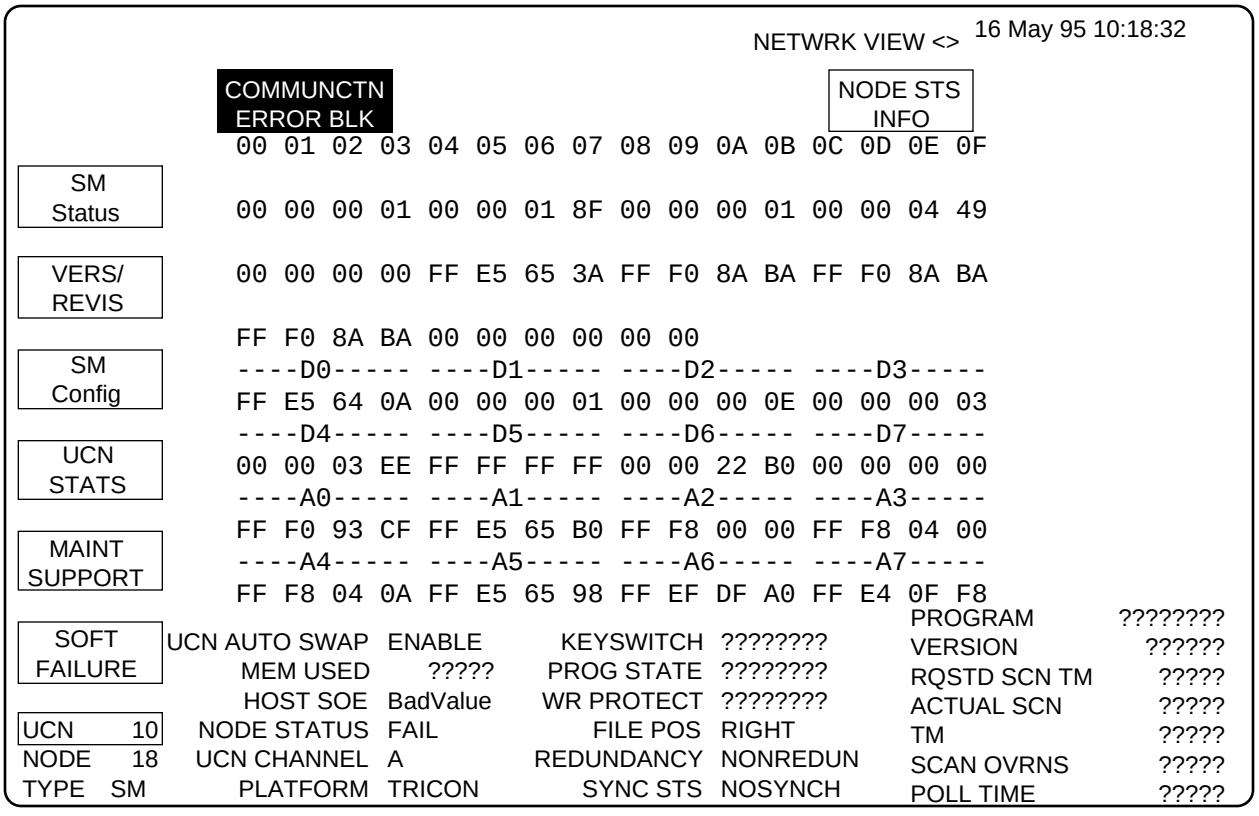
Continued on next page

Failed node

A failed node is seen at the Operator Station's System Status display, as FAIL or OFFNET. An SMM reset by its WatchDog Timer is displayed as momentarily OFFNET. It will return to an ALIVE state. Figure 3-5 shows the UCN Status display for a failed node.

ATTENTION Bring up this display when you have a failed or OFFNET node. However, do not attempt to interpret these numbers. Call your Honeywell Technical Assistance Center (TAC) personnel for assistance.

Figure 3-5 UCN Status Display for a Failed Node



Section 4 – Safety Manager Start-up and Shutdown

4.1 Cold Start-up

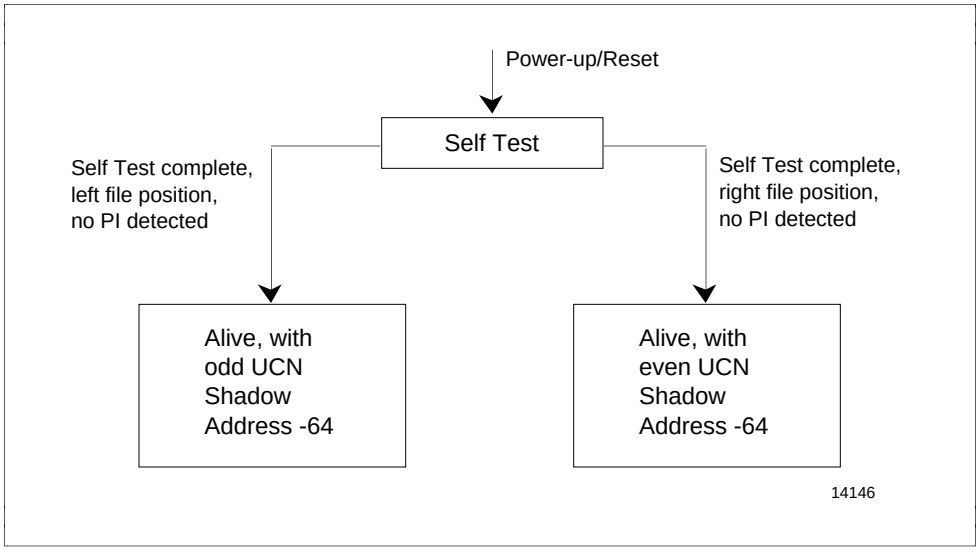
Section summary

This section contains the following topics:

Cold startup

Following power-up reset, the SMM will operate from Read Only Memory (ROM). It will perform self testing and then arrive at one of the two ALIVE states illustrated in Figure 4-1, depending on file position.

Figure 4-1 Cold Start-up ALIVE States



ATTENTION Before the SMM can enter the ALIVE state, a control program with the SMM configured must have been previously loaded by the TRISTATION into the TRICON.

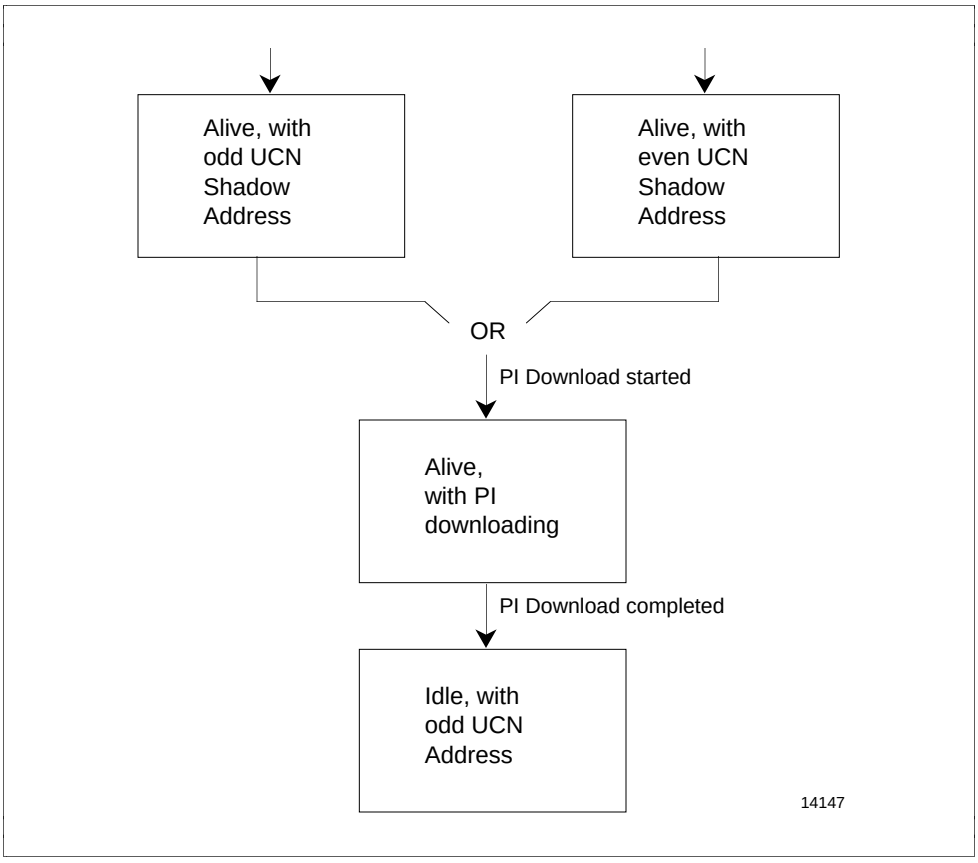
For information on TRICON start-up and shutdown, refer to Triconex's *TRICON Planning and Installation.*

Continued on next page

Downloading SMM personality

Next, the operator must select one of the two SMM nodes (from the UCN Status display) and initiate a Personality download.

Figure 4-2 SMM Personality Download



ATTENTION Repeat steps in Figure 4-2 to download second SMM. Note that the second SMM assumes the even UCN access.

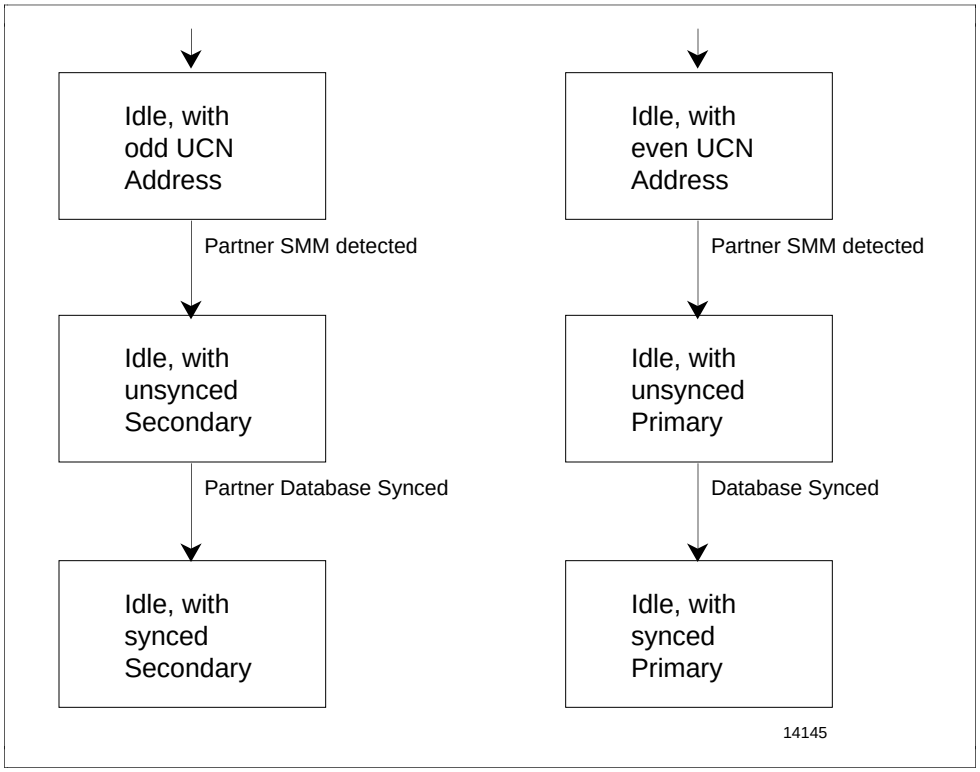
Continued on next page

Cold start-up—SMM idle state

When an SMM reaches the IDLE state, it begins searching for or communicating with a partner SMM. This process is carried out over the Private Link and UCN.

Once contact is made with a partner, Primary/Secondary states are resolved and the SMMs then move to synchronize their databases. This is illustrated in Figure 4-3.

Figure 4-3 Primary/Secondary Idle State Synchronization



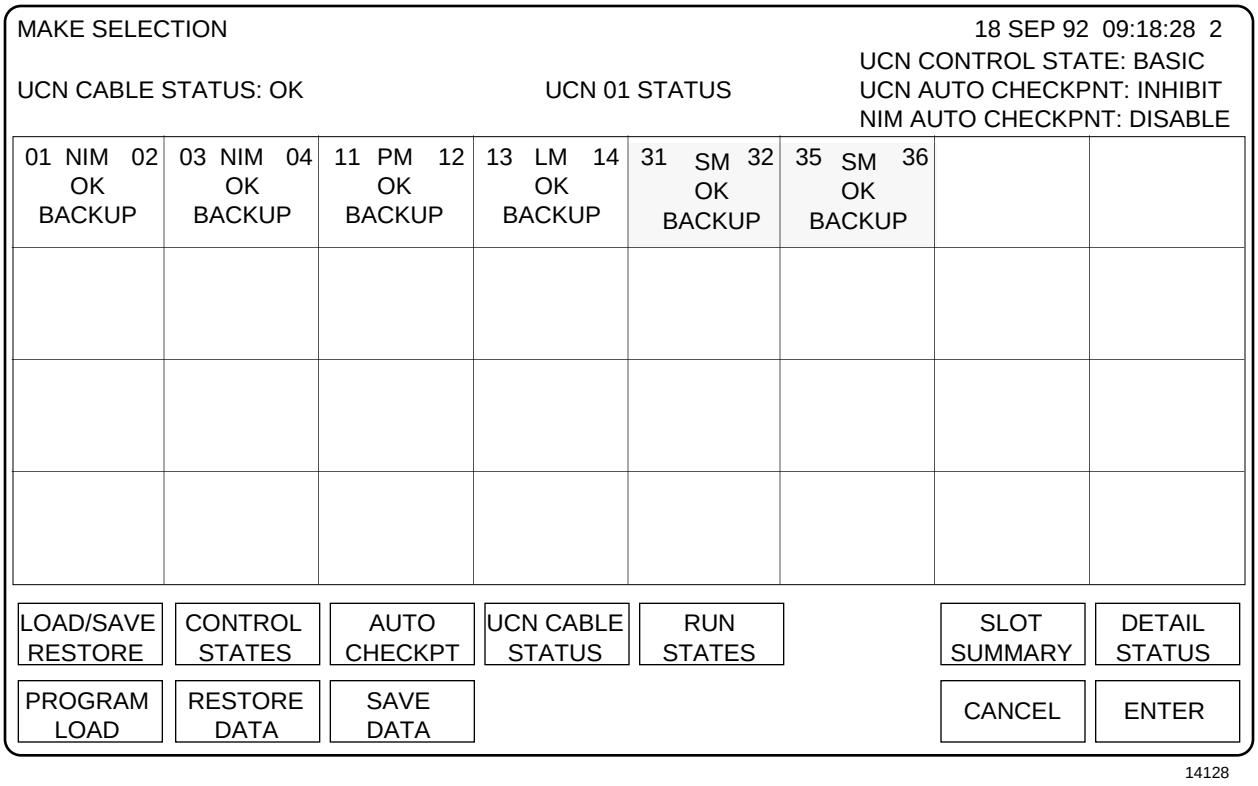
Continued on next page

Cold start-up—SMM idle state, continued

During Database Synchronization, the Primary suspends all normal operations involving its database. This Sync process requires less than two seconds to complete. During this completion time, any UCN parameter access requests are queued for later servicing.

Figure 4-4 shows UCN Status display once the SMMs have reached synchronization state. Note the “IDLE” or “OK” for the Primary and “BACKUP” for the Secondary.

Figure 4-4 SMM UCN Status Display Synchronized State



4.2 Warm Start-up

Warm start-up

Warm start-up is the condition where an SMM has retained its Personality (PI) and database through a power cycle. Therefore, the device is allowed to continue processing without operator intervention.

SMM idle/run state—warm start-up

With warm start-up following power-up reset, the SMM will operate from ROM to perform self testing. It then looks for the existence of a valid Personality and database and proceeds without operator intervention. The Personality will take control of the SMM platform and bring the system to the state it was in (IDLE or RUN) prior to loss of power, assuming conditions allow operation in that state to continue (e.g., keyswitch position).

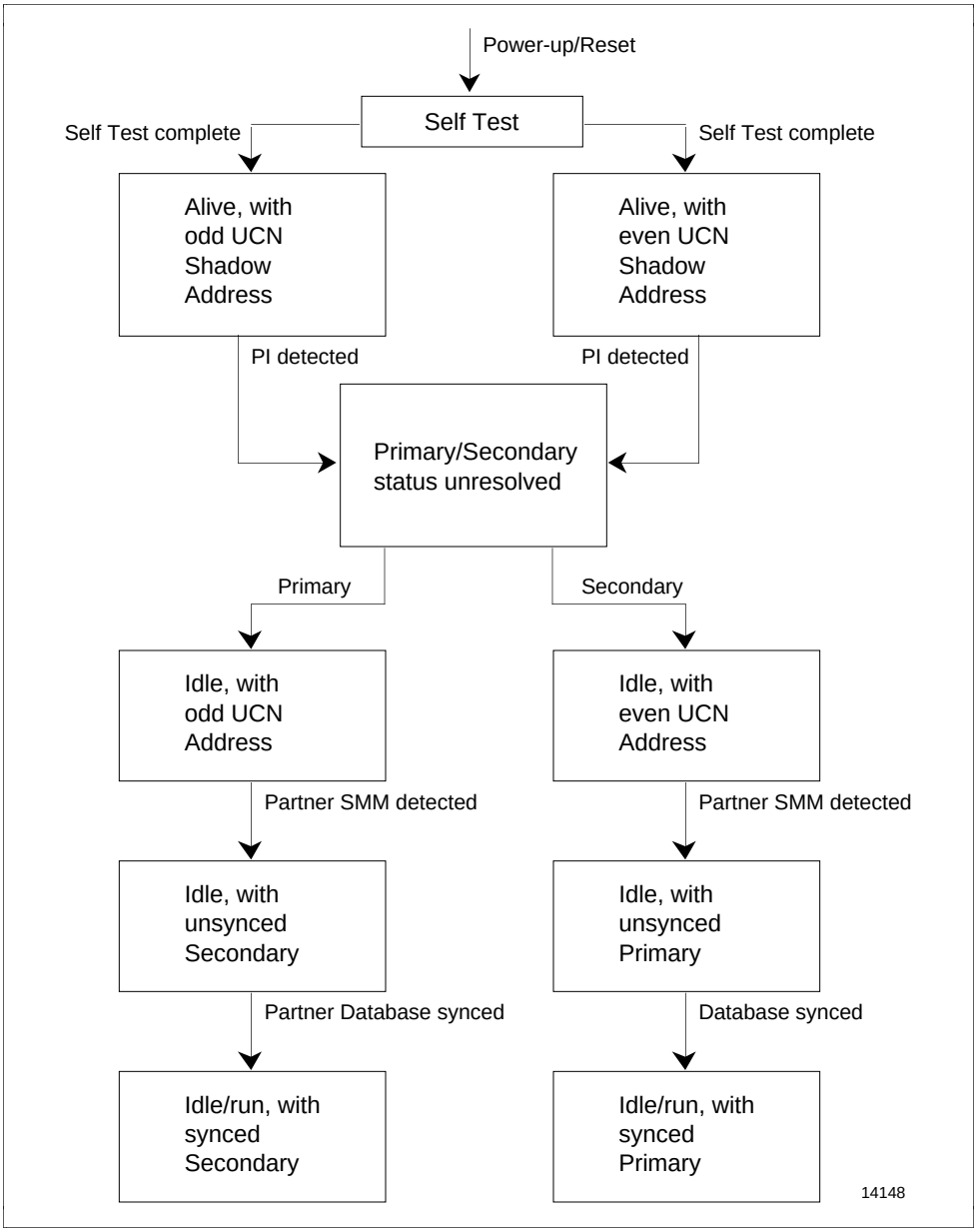
ATTENTION The new Secondary, when swapped, will not do self test (fast restart).

Continued on next page

SMM idle/run state—warm start-up, continued

Figure 4-5 illustrates the various steps for a warm start-up.

Figure 4-5 SMM Idle State—Warm Start-up



4.3 Shutdown

Shutdown

Shutdown returns an SMM to its ALIVE state. Shutdowns may be initiated from the Operator Station using the procedure outlined in Table 4-1.

Table 4-1 SMM Shutdown

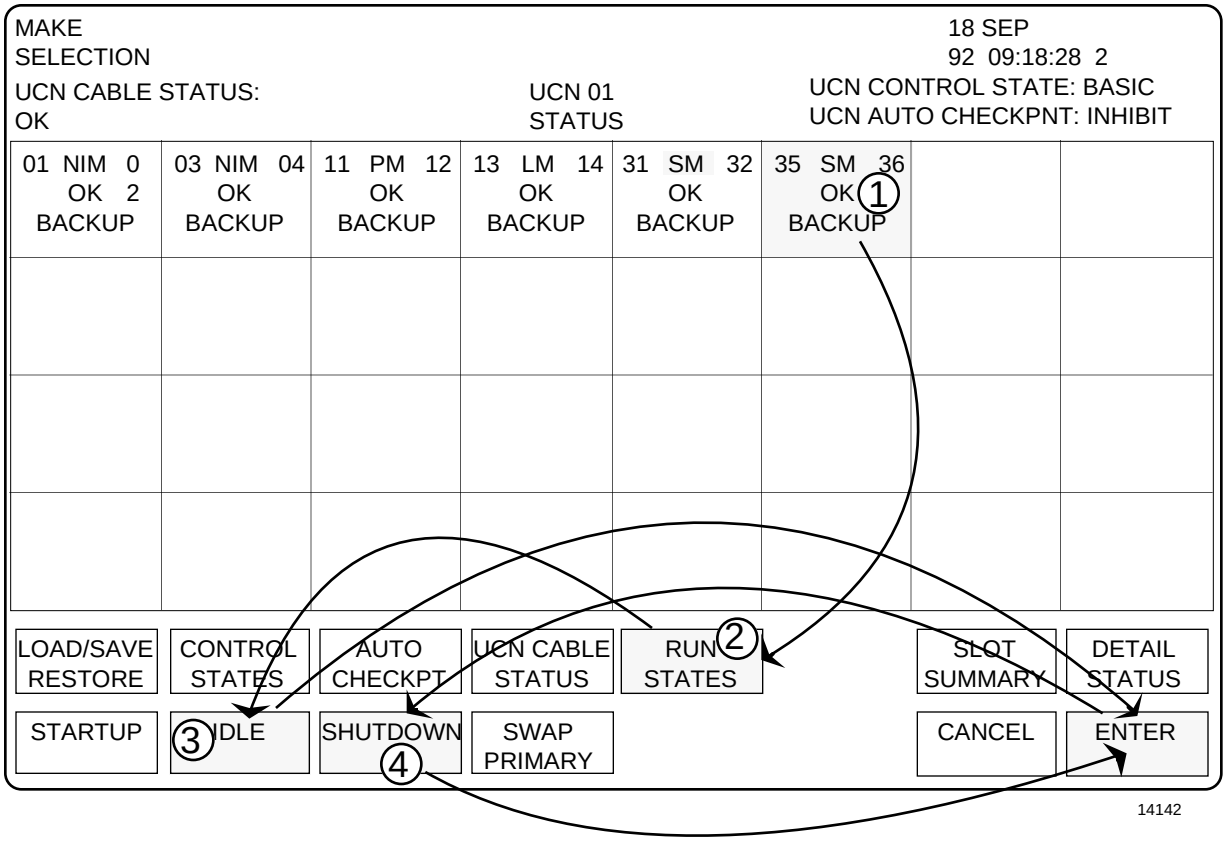
Step	Action
1	Select the targeted node from the screen shown in Figure 4-6.
2	Select the “RUN STATES” target.
3	Select “IDLE” target then select “ENTER.”
4	Select the “SHUTDOWN” target then select “ENTER.”

ATTENTION If the Shutdown command is received by a Primary that has a Synced Secondary, a No-Fault Switchover (without resync) will be executed prior to the shutdown.

UCN shutdown status display

Figure 4-6 shows the UCN Status display for SMM shutdown.

Figure 4-6 SMM Shutdown UCN Status Display



Section 5 – Performance Specifications

5.1 MPU Resource Allocations

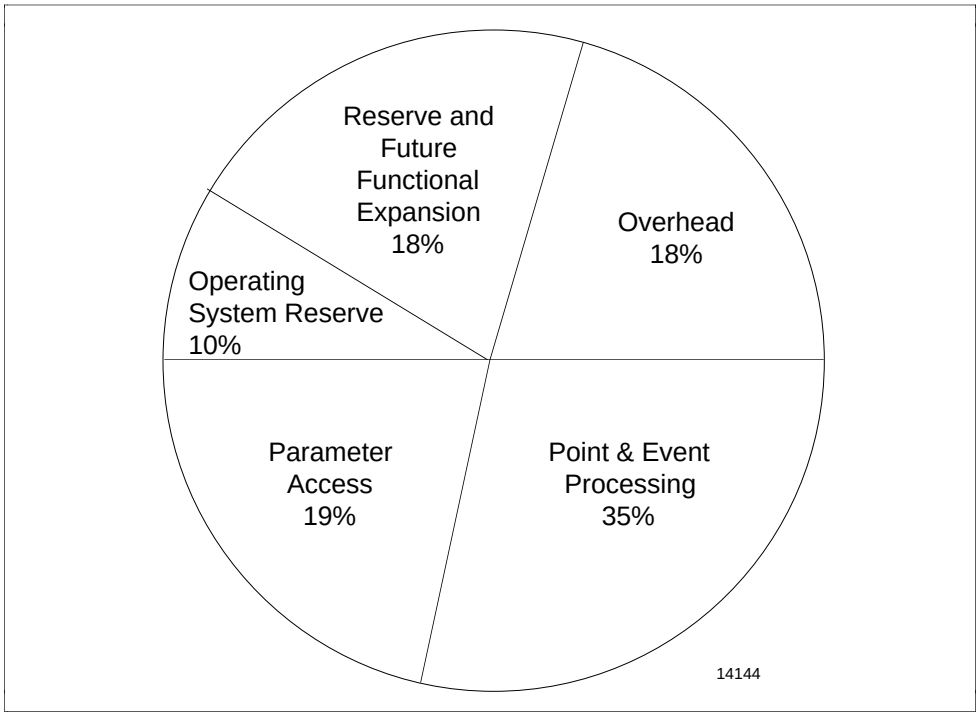
Section summary

This section contains the following topics:

Performance specifications summary

Figure 5-1 outlines the relative allocation of MPU resources to the major tasks and functions for the Safety Manager.

Figure 5-1 SM MPU Resource Allocation



Overhead

One of the resource allocations of the MPU that may need further explaining is overhead. Overhead includes the background functions required to support the SM node and SMM interface to the TRICON. It includes the following:

- TRICON backplane access,
- diagnostics and status, and
- redundancy and checkpointing.

5.2 Performance Statistics

Performance specifications

Table 5-1 outlines the performance specifications for the Safety Manager.

Table 5-1 Performance Specifications

Parameter	Specification
Point Processing	Scan rate: 1 sec. 0.5 sec.
UCN Parameter Access	800 read requests per second* 100 control writes per second
Database Synchronization	2 seconds for a maximum database of 150 Kbyte
Self-diagnostics	Every 60 seconds
Failover	5 seconds
Primary/Secondary Switchover and Point Process Priming	2 seconds
SOE Resolution	User program scan time
Minimum Configurable Scan Time	40 milliseconds** (Scan time must be equal to or exceed TRICON control program scan time)

* Represents a combined load of LCN (US, HM, AM, CM) and UCN (peer-to-peer) initiated request.

** The smallest increment of real time that can separate two consecutive SOE timestamped events.

5.3 Processing Units

Processing units for the SMM

Table 5-2 outlines the processing units for the SMM.

Table 5-2 Processing Units for the SMM

Point Type	Maximum Number of Points	Processing Units per Point
Analog Input	1000	10.2
Analog Output	1000	8.5
Digital Input	2000	2.5
Digital Output	2000	1.2
Digital Composite	652	11.1
Timer	1500	3.1
Logic	30	200

ATTENTION

- The 0.5 second scan rates will tend to lower the maximum number of points.
- Refer to Table 7-2 for processing-unit calculation.

Section 6 – NIM Processing

6.1 Estimating NIM Loading

Section summary

This section contains the following topics:

NIM processing load example

Table 6-1 gives an example of a NIM processing load estimate. In this example, the total induced load is 335, which is 33.5% of the maximum load allowed for a NIM.

Table 6-1 NIM Processing Load Estimator

Load Sources	Units to be Entered in Number Column	Number	Load Factor	Induced Load
PM/LM/SM Induced Load				
PMs, LMs and SMs on UCN	Number of PMs, LMs and SMs on UCN	1	10	10
US Induced Load				
Universal Stations	Number principally accessing this NIM	3	15	45
Schematic Displays on those USs	Number principally accessing this NIM	1	30	30
HM Induced Load				
History Modules	Number principally accessing this NIM	1	30	30
Checkpointing	Number of HMs checkpointing this NIM	1	70	70
AM and CG Induced Loads				
AMs with 68020 microprocessor	Number principally accessing this NIM	1	150	150
AMs with 68000 microprocessor	Number principally accessing this NIM	0	95	0
Computer Gateways	Number principally accessing this NIM	0	60	0
			Total Induced Load:	**335**
			Maximum Allowable Load:	**1000**
			% of Maximum Allowable Load:	**33.5%**

Continued on next page

Estimating NIM processing loading

The NIM processing load estimate is calculated as outlined in Table 6-2.

Table 6-2 NIM Processing Load Estimate Calculation

Step	Action
1	Multiply the value you entered in the Number column in Table 6-1 by the factor in the Load Factor column.
2	Enter the results in the Induced Load column.
3	Total the values in the Induced Load column.

ATTENTION You should make such an estimate for each NIM in your system.

Considerations for NIM load calculation

You should keep the following factors in mind when calculating the NIM processing load.

- Count redundant node pairs (NIMs, AMs, PMMs, LMs and SMs) as one.
- The load factor for schematic displays is based on a schematic with 250 parameters that is principally accessing this NIM (four second update intervals).
- The AM load factor is based on a fully-loaded AM accessing data from this NIM.
- If you have several NIMs, you might consider using a spread sheet on a personal computer to do your calculations.

6.2 Assessment of NIM Processing Load

NIM processing load categories

Table 6-3 outlines the NIM processing load categories.

Table 6-3 NIM Processing Load Categories

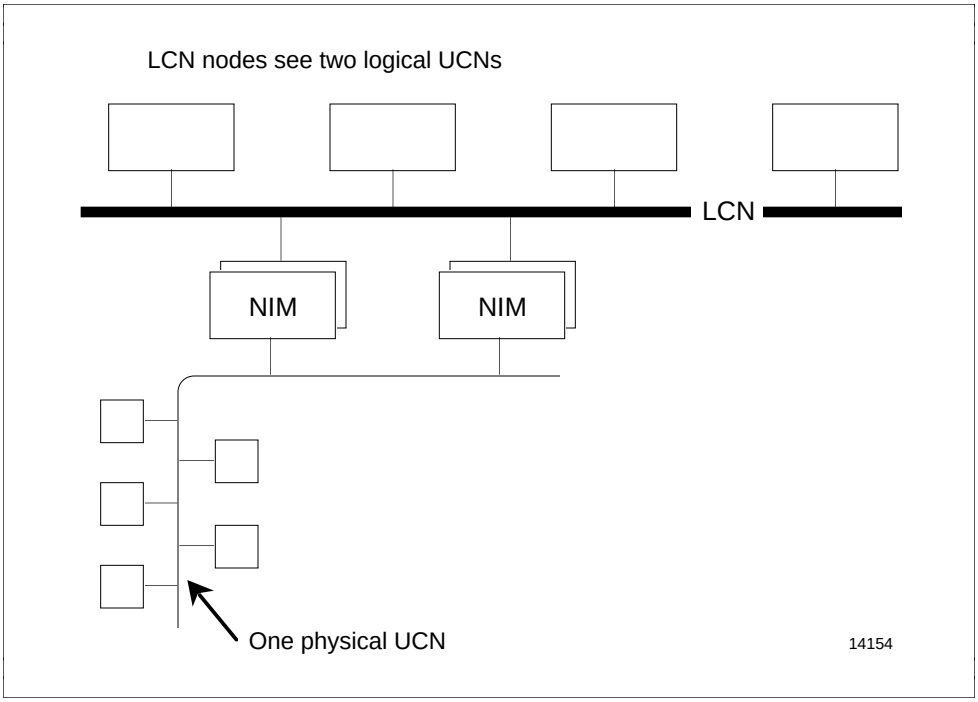
Induced Load	Performance Rating	Result
750 (75%)	Performance as Specified	Will perform as specified under all actual system use conditions.
750 to 1000 (75% to 100%)	Marginally Acceptable	Display of information from this NIM and its reporting of events may occasionally be sluggish, especially during a process upset or a peak load such as multiple point loading.
1000 (100%)	Overloaded	Should a failover to the backup NIM or some other system upset occur, the view to the process may be temporarily lost.

6.3 “Remote” NIM Sharing Processing Load

Adding NIMs to the UCN

An additional NIM (redundant NIM pair) can be added to the UCN and the LCN to share the processing load with another NIM. Figure 6-1 illustrates the new UCN configuration with an additional NIM.

Figure 6-1 Additional NIMs on UCN Configuration



NIM assignments

From the LCN viewpoint, the two NIMs (two redundant NIM pairs) are on separate process networks, even though they are connected to the same physical UCN. NIM assignments are as follows:

- NIM 1 (configured as ThisNIM)—assigned to process network n (n is in a range from 1 to 20; each UCN and each Data Hiway is one process network).
- NIM 2 (configured as RemotNIM)—assigned to process n+1.

ATTENTION Assignment of network numbers is arbitrary, but consistent, logical assignment simplifies operating practices. See Figure 6-2.

Continued on next page

Implementation of two logical process networks

To implement two logical process networks, you must follow the procedure outlined in Table 6-4.

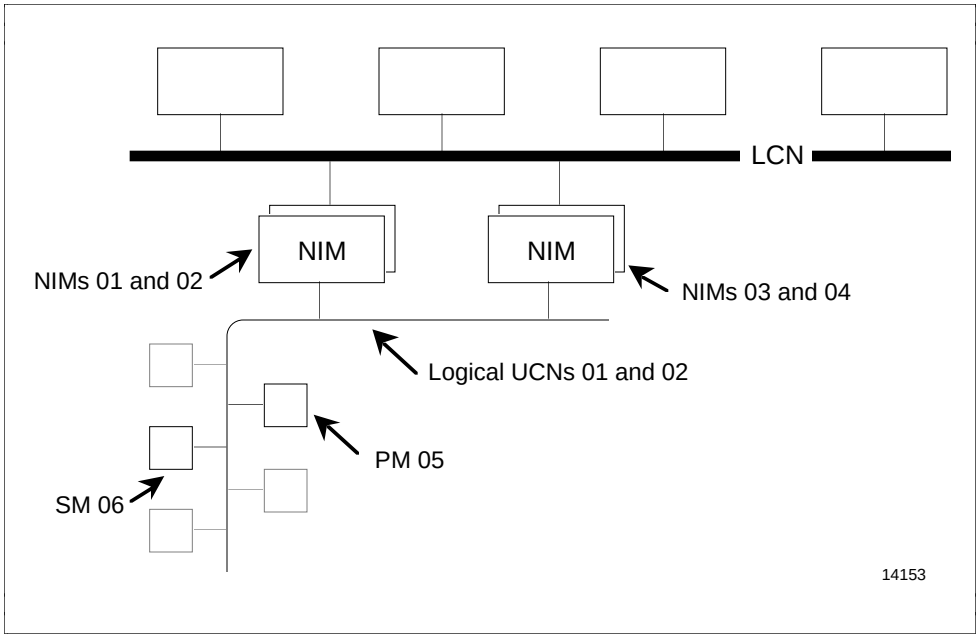
Table 6-4 Implementation of Two Logical Process Networks

Step	Action
1	ThisNIM and RemotNIM and their process networks must be defined in the Network Configuration File (NCF) through the Engineering Personality’s LCN NODES activity.
2	All UCN nodes, including NIMs, must be defined on both process networks by building UCN entities (NIM points) and node-specific entities (box points).
3	In the UCN node entities, approximately half of the nodes on each process network are configured with NODEASSN = ThisNIM and the remainder with NODEASSN = RemotNIM.
4	Each node assigned as ThisNIM on process network n is assigned as RemotNIM on n+1, and each node assigned as ThisNIM on process network n+1 is assigned as RemotNIM on network n.

NIM addition example

Figure 6-2 gives an example of an additional NIM on a UCN configuration.

Figure 6-2 Specific Example of Additional NIM on a UCN



Continued on next page

NIM addition example, continued

For the UCN node numbers in Figure 6-2, you would build the UCN node and node-specific entities as outlined in Table 6-5.

Table 6-5 Building UCN Node and Node-specific Entities

Node	UCN	UCN Entity Name	NODEASSN	Node-Specific Entity Name
NIM 01	01	$NM01N01	ThisNIM	N/A
NIM 02	01	$NM01N02	ThisNIM	N/A
NIM 03	01	$NM01N03	RemotNIM	N/A
NIM 04	01	$NM01N04	RemotNIM	N/A
PM05	01	$NM01N05	ThisNIM	$NM01B05
SM06	01	$NM01N06	RemotNIM	$NM01B06
NIM 01	02	$NM02N01	RemotNIM	N/A
NIM 02	02	$NM02N02	RemotNIM	N/A
NIM 03	02	$NM02N03	ThisNIM	N/A
NIM 04	02	$NM02N04	ThisNIM	N/A
PM05	02	$NM02N05	RemotNIM	$NM02B05
SM06	02	$NM02N06	ThisNIM	$NM02B06

Continued on next page

Operational considerations for two logical NIMs

Take into account the following considerations when you have two logical process networks (NIMs).

- Use of the SAVE DATA target to checkpoint data from the UCN nodes—The restoration of checkpoint data to the nodes can be accomplished only from the UCN Status display. For the process network, the nodes are assigned to (NODEASSN = ThisNIM).
- If you try data restoration from the wrong display, a "node assignment" error message appears. If some of the points in a UCN node are assigned to process network n+1, you will have to use SAVE DATA twice, once for each UCN Status display.
- For automatic checkpointing to save all data—you must enable it through the UCN Status displays for both process networks.
- Alarming, message transfers and event-initiated processing are handled by the NIMs and no special operational considerations are required.
- If SMM memory is corrupted, a checksum error will be detected.

Operational considerations for two logical UCNs

Take into account the following considerations when building process points to reside on two logical UCNs.

- Assign approximately equal numbers of points to each UCN (parameter NTWKNUM).
- Assign points that use peer-to-peer communication to the same UCN.

Section 7 – Building UCN and Node-specific Points

7.1 UCN Point Building

Section summary

This section contains the following topics:

UCN point building summary

One UCN point must be built for each node on the UCN. This includes each NIM and SM (non-redundant and redundant).

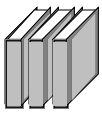
The UCN and LCN points are reserved entities (see Subsection 2.1 of the Data Entry Builder Manual). These entities must be built and loaded before data points can be loaded into the UCN nodes.

UCN point building procedure

UCN points are built with the Data Entity Builder. Table 7-1 outlines the procedure.

Table 7-1 UCN Point Building

Step	Action
1	Select NETWORK INTERFACE MODULE on the Engineering Main Menu.
2	Select UCN NODE CONFIGURATION.
3	Select NODE SPECIFIC CONFIGURATION to access the Parameter Entry Displays (PEDs) used to build them.



For information about the values to be entered, refer to the *Safety Manager Module Parameter Reference Dictionary* in the Implementation Safety Manager binder.

Continued on next page

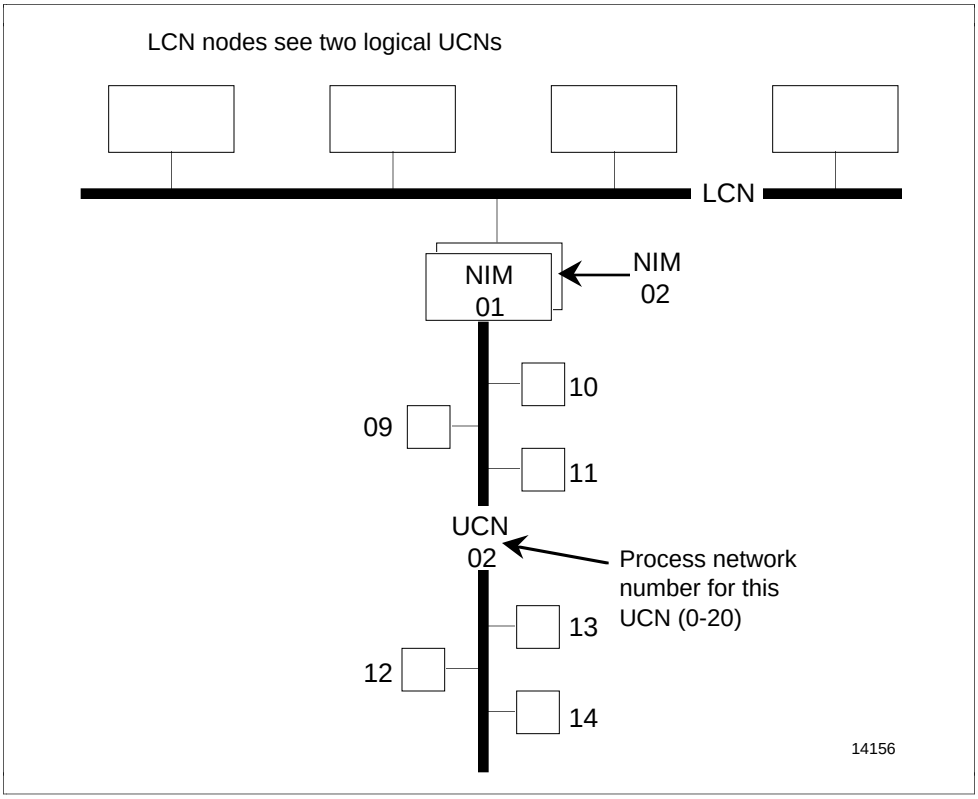
UCN point building example

The example listed below shows how reserved entities would be built for the UCN. It will reference Figure 7-1.

EXAMPLE:

UCN Node	UCN Point	Node-Specific Point
NIM, UCN node no. 1	$NM02N01	N/A
NIM, UCN node no. 2	$NM02N02	N/A
SM (or PM, LM), node no. 3	$NM02N03	$NM02B03

Figure 7-1 UCN Node Configuration

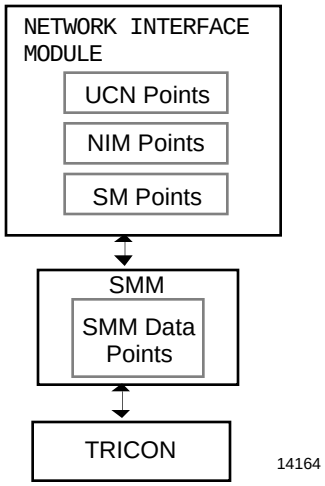


7.2 Node-specific Point Building

Node-specific point building summary

You must build node-specific points for each SM, including all redundant pairs on the UCN. Figure 7-2 shows where the node-specific SM data points information resides within the implementation scheme.

Figure 7-2 SM Implementation Dependencies



SMM database

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.

Relay ladder logic database

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.

ATTENTION Most diagnostic information that is provided in the TRICON is available at the US.

Continued on next page

Determining total SMM processing units

6000 is the maximum Processing Units for the SMM. Before building point displays, it is important that you determine your target maximum point counts and Processing Units. This can be done using Table 7-2.

Table 7-2 Target Maximum Point Counts and Processing Units

Point Type	Maximum Allowable Point Count	Processing Unit Value Per Point	X	Number or Points Desired	=	Total Point Processing Units
Digital Input 0.5 sec. digital scan	2000	2.5	X	_____	=	_____
1.0 sec. digital scan		1.25	X	_____	=	_____
Digital Output 0.5 sec. digital scan	2000	1.2	X	_____	=	_____
1.0 sec. digital scan		0.6	X	_____	=	_____
Digital Composite 0.5 sec. or 1.0 sec. digital scan	652	11.1	X	_____	=	_____
Analog Input 0.5 sec. analog scan	600	10.5	X	_____	=	_____
1.0 sec. analog scan	1000	5.25	X	_____	=	_____
Analog Output 0.5-sec. analog scan	1000	8.5	X	_____	=	_____
1.0 sec. analog scan		4.25	X	_____	=	_____
Logic 0.5 sec. or 1.0 sec. digital scan	30	200	X	_____	=	_____
Timer 0.5 sec. or 1.0 sec. digital scan	1500	3.1	X	_____	=	_____
				POINT PROCESSING TOTAL		_____

ATTENTION ***Please note the following:***

- 0.5 sec. digital scan when scanrate = AR1DT2 or AR2DT2.
  1.0 sec. digital scan when scanrate = AR1DT1.
  0.5 sec. analog scan when scanrate = AR2DT2.
  1.0 sec. analog scan when scanrate = AR1DT2 or AR1DT2.
- Point Processing total must be 6000 or less to be valid.
- FLAG and NUMERIC points use a fixed amount of processing overhead (PU = 0) and therefore are not required to be calculated into the Point Mix determination. You can configure as many as:
  – 2000 Flag points
  – 1000 Numeric points

ATTENTION

- This page may be reproduced for use as a configuration worksheet.
- LC overruns will occur if you are operating at or near 500 ms. To avoid this, the Logic Controller scan time should be less than the SMM scan time.

Continued on next page

Node-specific building displays

Figures 7-3 and 7-4 show the node-specific building displays for the US.

Figure 7-3 Node-specific Building Displays - Screen 1

PED >>>>>> POINT : $NM10B61 UNIT: SY

NODE – SPECIFIC CONFIGURATION (FOR SM)

NUMBER OF ANALOG INPUT SLOTS	(NAISLOT)	800
NUMBER OF ANALOG OUTPUT SLOTS	(NAOSLOT)	20
NUMBER OF DIGITAL INPUT SLOTS	(NDISLOT)	1200
NUMBER OF DIGITAL OUTPUT SLOTS	(NDOSLOT)	100
NUMBER OF LOGIC SLOTS	(NLOGSLOT)	10
NUMBER OF DIG. COMPOSITE SLOTS	(NDCSLOT)	300
DIG. COMPOSITE NONE STATE	(NONETXT)	NONE
NUMBER OF NUMERICS	(NNUMERIC)	1000
SM START ADDR OF NUM ARRAY	(NNLSBA)	41001

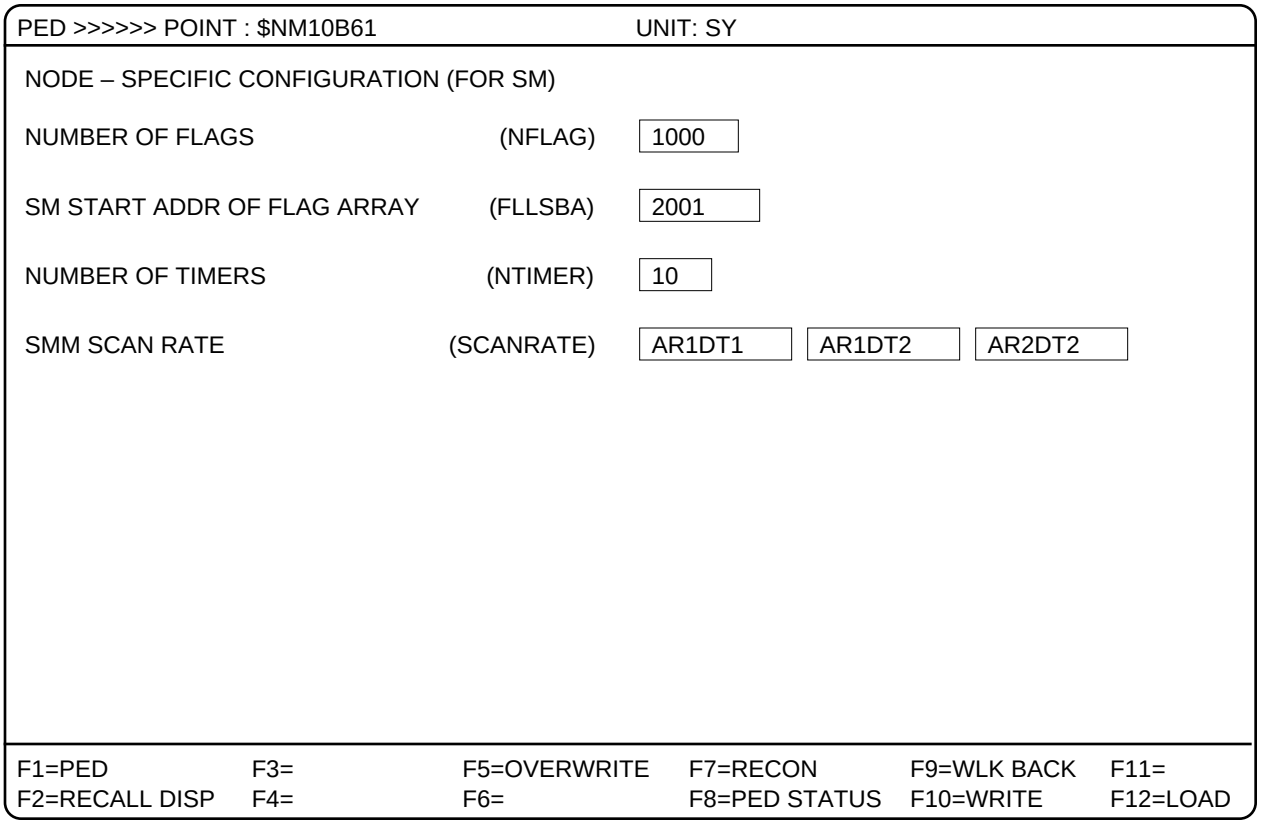
F1=PED	F3=	F5=OVERWRITE	F7=RECON	F9=WLK BACK	F11=
F2=RECALL DISP	F4=	F6=	F8=PED STATUS	F10=WRITE	F12=LOAD

14140

Continued on next page

Node-specific building displays, continued

Figure 7-4 Node-specific Building Displays - Screen 2



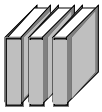
7.3 Box Configuration

Data point building

Data points are built with the Data Entity Builder. Table 7-3 outlines the procedure you should use.

Table 7-3 Data Point Building

Step	Action
1	Select NETWORK INTERFACE MODULE from the Engineering Main Menu.
2	Select PROCESS POINT BUILDING.
3	Choose the type of point(s) desired (i.e., Analog, Digital, Digital Composite, Timer, Flag, Numeric Logic).
4	Select point type options desired. Configure SOE for DI points if desired. Refer to the *Safety Manager Module Control Functions* manual for information about each point type. **ATTENTION** SMM output points cannot be mapped to TRICON outputs. TRICON programming (i.e., RLL) will be required to affect real output control and can only be done through the TRISTATION.
5	Select the Parameter Entry screen displays. Enter in parameters. Refer to *Safety Manager Module Parameter Reference Dictionary* for parameter details.



Refer to the *Safety Manager Module Installation Guide* in this binder for US configuration of SMM data points.

Loading points

Points are loaded by selecting appropriate targets on the Data Entity Builder's Command Menu or from the Parameter Entry display by pressing a function key.

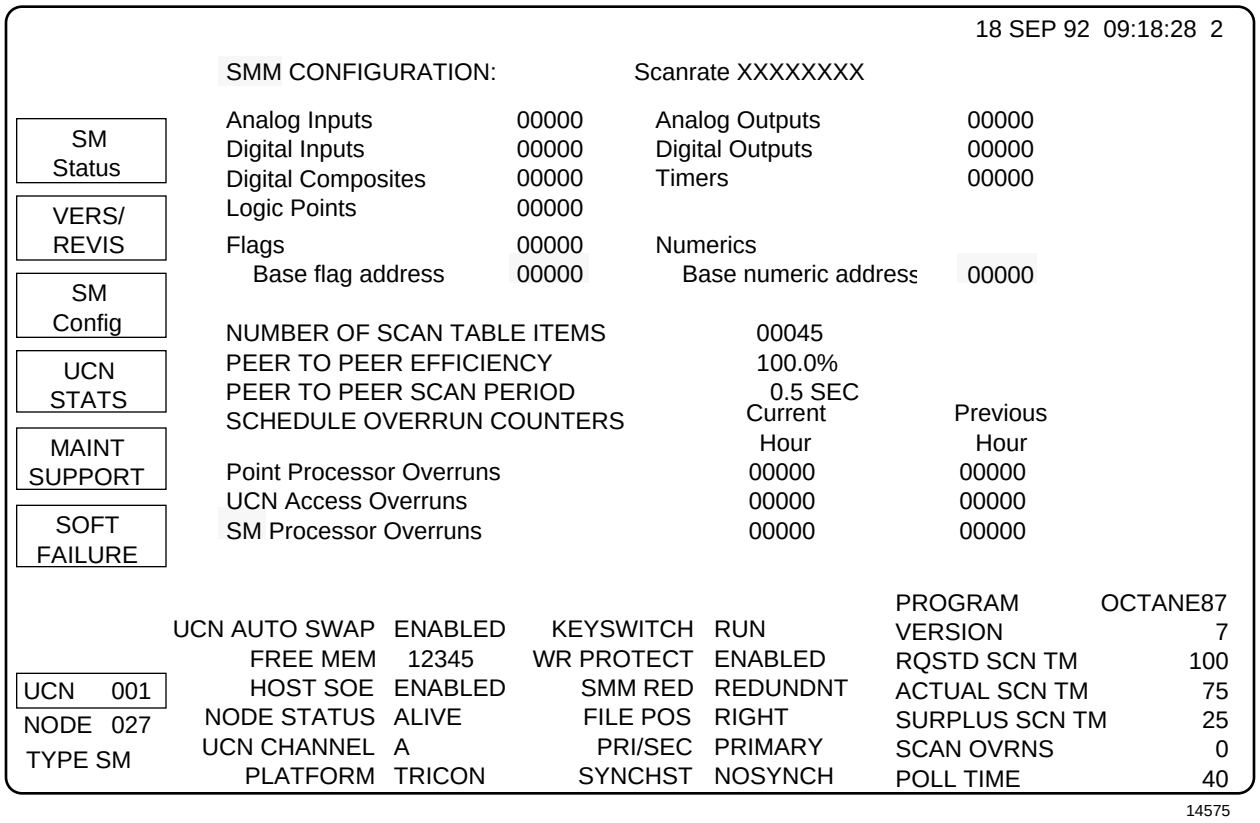
ATTENTION Points can only be loaded when the designated slot is in the inactive state.

Continued on next page

Viewing SMM point configuration

Figure 7-5 shows the SMM Configuration display which provides a view of the box configuration (summary of the quantity of the various point types).

Figure 7-5 Point Types—SMM Configuration Display



Section 8 – Error Handling

8.1 Soft Failures

Section summary

This section contains the following topics:

Soft failures

Soft failures are situations where control and process view are maintained, but a fault has jeopardized system integrity.

A Safety Manager softfail will result for numerous reasons.

Softfail descriptions

Table 8-1 lists the types of softfails that may be encountered.

Table 8-1 Softfail Descriptions

Code	Journaled Text	Text Displayed on SMM Diagnostic Displays	SMM Interpretation and/or Comments
19	UCNPRSFL	Pri Cannot Talk to Sec on UCN	SMM has the ability to maintain Database Synchronization over a Private Link and use the UCN as an alternate path for checking the status of their partner.
20	UCNSCPFL	Sec Cannot Talk to Pri on UCN	SMM has the ability to maintain Database Synchronization over a Private Link and use the UCN as an alternate path for checking the status of their partner.
21	NOSYNCH	Secondary Not Synched	Loss of SMM Redundancy.
22	UIMBATFL	SMM Battery Failure	Loss of SMM (UCN interface module) battery. Subsequent loss of SM power will result in loss of SMM database.
34	UCNOVRUN	UCN Overrun	SMM unable to prefetch data from remote nodes (peer-to-peer inputs).
35	PPXOVRUN	Point Processor Overrun	SMM point scanning is lagging behind schedule.

Continued on next page

Softfail descriptions, continued

Table 8-1 Softfail Descriptions, Continued

Code	Journaled Text	Text Displayed on SMM Diagnostic Displays	SMM Interpretation and/or Comments
51	PLCOVRUN	LC Overrun	LC data collection (LC Prefetch) lagging behind Point Processing or failed altogether. LC overruns occur if you are operating at or near 500 ms. Adjust the configuration so that the Logic Controller scan time is less than the SMM scan time.
54	LCLLNOSC	LC Not Scanning	SMM Point Processing requires the Logic Controller to scan its inputs and its user program.
55	LCSYSERR	Main Processor Failure	This is only a soft failure if at least one other MP remains operational.
59	LCBATTFL	LC Battery Failure	One or both LC batteries have failed.
63	LCSIOMOL	LC Comm or I/O Card Fault	TRICON System Aliases are signaling an I/O fault.
80	UIMTSFLT	SMM Time Synch Failure	Set by an SMM upon detection of a UCN Time Sync failure. Causes include: • UCN Time Sync hardware/software failure. • At least ten minutes since last UCN Time Sync.
81	LCTSFLT	LC Time Synch Failure	Set by an SMM upon detection of a Logic Controller Time Sync error. Causes include: • TRICON Time Sync hardware failure. • TRICON Time Sync command processing failure.

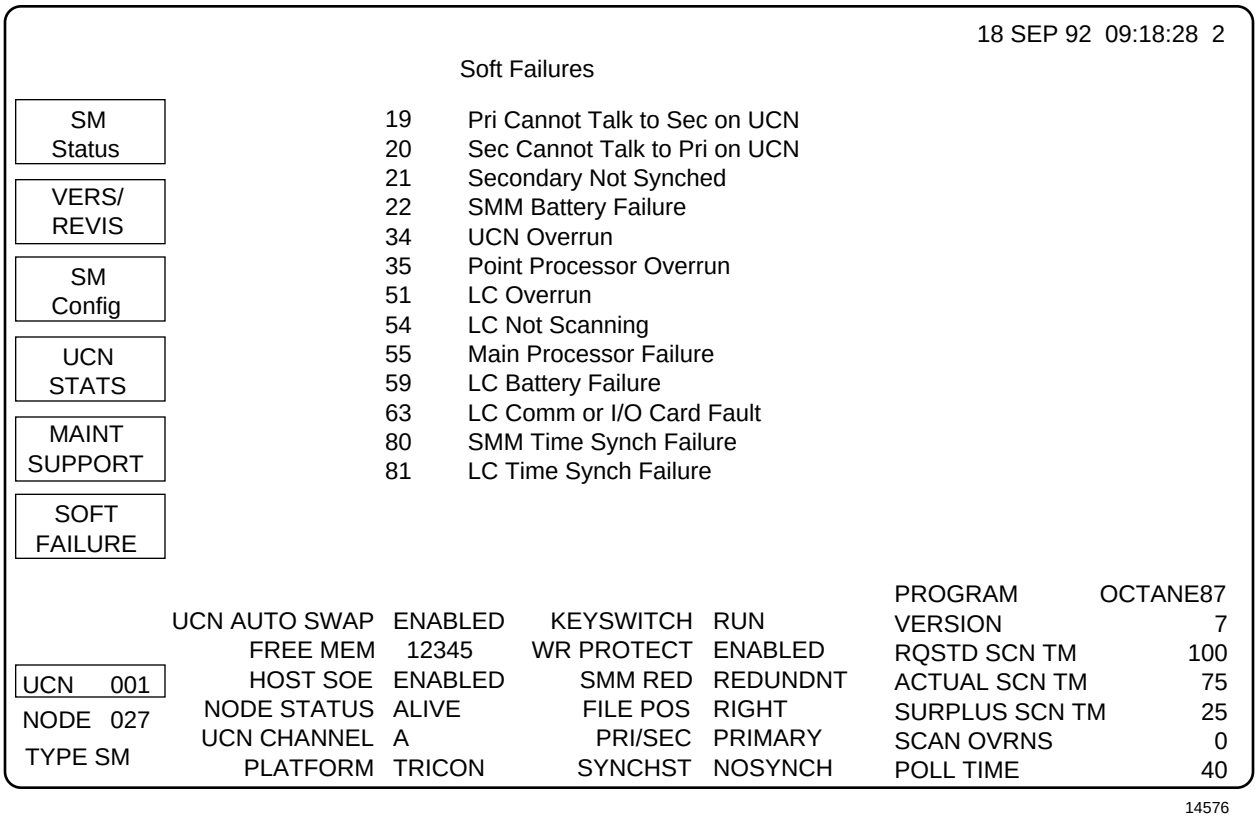
Continued on next page

Soft failures US display

Figure 8-1 shows a US display which provides you with the various Safety Manager soft failures and their corresponding error codes.

ATTENTION Active soft failures will be highlighted.

Figure 8-1 US Display—Soft Failures



14576

Private link softfail

Should the Private Link fail, it will be treated as a softfail. Because it is a softfail, it will allow the two SMMs to maintain a view of the process. Upon Private Link softfail the SMMs will

- resolve Primary/Secondary status based upon UCN communications or SMM preference,
- switch to the UCN for Sync and Flush operations.

ATTENTION This is done to maintain redundancy and to allow for the installation of a replacement unit without the loss of the database.

Continued on next page

Keep alive

WatchDog Timer expiration results in a hardware restart. Keep Alive mechanisms will be used for TRICON and Private Link interfaces.

Since the SMM is applied to a TMR architecture, the failure of a link to a TRICON MP will not necessarily dictate a failover. Instead, the SMMs will attempt to isolate the failure and maintain the most effective interface.

Redundant SMMs will channel switchover request through the UCN, Private Link, and Comm Bus to provide security against failures in any one or two of those links.

8.2 Hard Failures

Hard failures summary

Hard failures will result in SMM shutdown (to the FAIL state, ALIVE state, or total reset). Hard failures include the following:

- component failure,
- program or database failure.

Redundant SMM/Time Sync hardware failures

For redundant SMMs, Time Sync hardware failures will trigger consideration of the need for a failover. A failover may not occur if the Secondary is also partially failed (i.e., the SMMs will attempt to keep the most effective SMM as Primary).

ATTENTION Under no circumstances is a non-redundant SMM hard failed for time sync problems.

Time sync hardware fault compensation

Total loss of either UCN or TRICON Time Sync functions will result in shutdown of SM Time Sync. Loss at UCN Time Sync is not considered a "total" loss if less than ten minutes in duration.

Crash codes

Fail (crash) situations involve a large number of possible error codes. Contact the Technical Assistance Center (TAC) for help in identifying the causes of such failures.

8.3 Point Configuration Errors

Errors in configuring points

The SMM will only recognize LC Aliases previously configured within the TRICON. Table 8-2 lists configuration errors for the Safety Manager.

Table 8-2 Configuration Errors

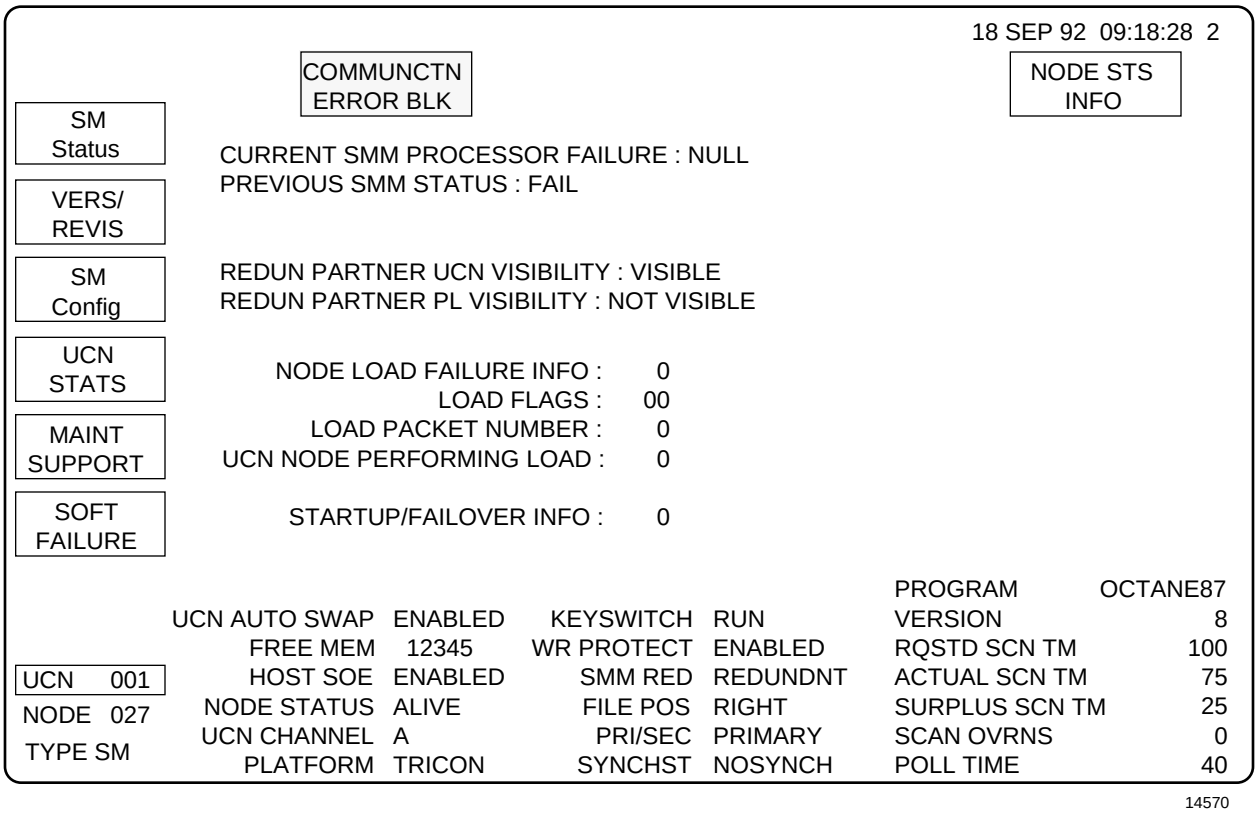
Error	Description
ILLEGAL VALUE	Attempted to write a TRICON hardware addressing parameter (e.g., PLCADDR, LODSTN, CCSRC, ILCxxxxx, etc.) which specifies an Alias not available within the host TRICON.
READ ONLY	Response to attempts to write to a read-only SM point.
CONFIGURATION MISMATCH	An invalid LC alias (PLCADDR). Attempts to change PTEXECST to ACTIVE will be denied.

8.4 Communication Errors

US display for communication errors target

Figure 8-2 is the US display which allows you to access the Communication Error Block screen. To do this, you need to select the "COMMUNCTN ERROR BLK" target.

Figure 8-2 US Display—COMMUNCTN ERROR BLK Target



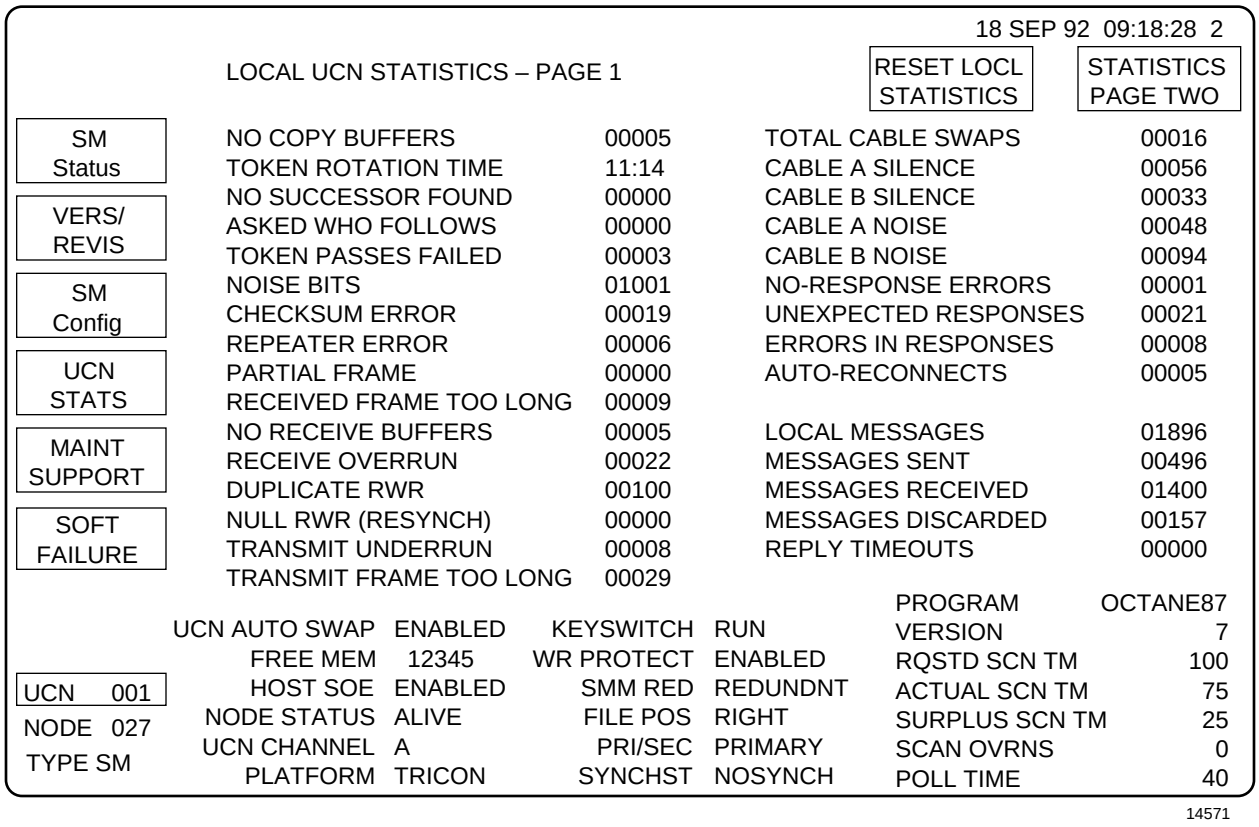
14570

Continued on next page

US display showing UCN statistics

Figure 8-3 shows the US Communication Block Error display which lists the various UCN communication error statistics, along with other UCN statistics. The values given are samples of what might be expected.

Figure 8-3 US Display—Communication Block Error Screen



UCN addressing errors

A Safety Manager UCN Address is configured using the TRISTATION. Range checking within the TRISTATION is assumed (1-63, odd addresses only). The left/right module placement within a given slot determines odd/even shadow addressing. It is therefore impossible for an SMM to operate with an invalid UCN address. However, there is no protection against duplicate use of a UCN address.

Index

M

N

O

P, Q

R

S

Index

T

U

V

W, X, Y, Z

READER COMMENTS

Honeywell's IAC Automation College welcomes your comments and suggestions to improve future editions of this and other publications.

You can communicate your thoughts to us by fax, mail, or toll-free telephone call. We would like to acknowledge your comments; please include your complete name and address.

BY FAX: Use this form; and fax to us at (602) 313-4108.

BY TELEPHONE: In the U.S.A. use our toll-free number 1*800-822-7673 (available in the 48 contiguous states except Arizona; in Arizona dial 1-602-313-5558).

BY MAIL: Use this form; detach, fold, tape closed, and mail to us.

Title of Publication: **Safety Manager Module Implementation Guidelines** Issue Date: **4/96**

Publication Number: **SM11-500**

Writer: **Vernadine Merrick**

COMMENTS: _____

_____

_____

_____

_____

_____

_____

_____

_____

RECOMMENDATIONS:_____

_____

_____

_____

_____

_____

_____

_____

NAME _____ DATE _____

TITLE _____

COMPANY _____

ADDRESS _____

CITY _____ STATE _____ ZIP _____

(If returning by mail, please tape closed; Postal regulations prohibit use of staples.)

Communications concerning technical publications should be directed to:

Automation College
Industrial Automation and Control
Honeywell Inc.
2820 West Kelton Lane
Phoenix, Arizona 85023

FOLD FOLD

From: _____

_____

_____

NO POSTAGE
NECESSARY
IF MAILED
IN THE USA

BUSINESS REPLY MAIL

FIRST CLASS **PERMIT NO. 4332** PHOENIX, ARIZONA

POSTAGE WILL BE PAID BY ....

Honeywell

Industrial Automation and Control
2820 West Kelton Lane
Phoenix, Arizona 85023

Attention: Manager, Quality

FOLD FOLD

Cut Along Line

Additional Comments:

Honeywell

Industrial Automation and Control
Honeywell Inc.
16404 North Black Canyon Highway
Phoenix, Arizona 85023

Helping You Control Your World