Honeywell

FSC Safety Manager
Implementation Guidelines

for use with the Honeywell FSC System

Release 400

FS11-500

TotalPlant®

Honeywell

Implementation
FSC Safety Manager

FSC Safety Manager
Implementation Guidelines

for use with the Honeywell FSC System
Release 400

FS11-500
09/96

TotalPlant®

Copyright, Notices, and Trademarks

Revision 03 – September 24, 1996

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 mplementation of the FSC Safety Manager Module for use with the Honeywell FSC system Release 400. Use this document as an informational source, a guide and reference to implementation requirements, and for FSC Safety Manager operational considerations.

All references in this manual to "FSC Safety Manager" or "FSC Safety Manager Module" pertain only for use with the Honeywell FSC system.

Table of Contents

Figures

Tables

Acronyms

AM.....Application Module
APM.....Advanced Process Manager
APMM.....Advanced Process Manager Module
CG.....Computer Gateway
CL.....Control Language
CM.....Computing Module
CP.....Central Part
CP.....Control Processor
CP.....Control Program
CPU.....Central Processing Unit
DCS.....Distributed Control System
DEB.....Data Entity Builder
EPROM.....Erasable Programmable Read-Only Memory
FLD.....Functional Logic Diagram
FSC.....Fail Safe Control
FSC-DS.....FSC Development System
FSC-SM.....FSC Safety Manager
FSC-SMM.....FSC Safety Manager Module
HM.....History Module
I/O.....Input/Output
LCN.....Local Control Network
LM.....Logic Manager
NCF.....Network Configuration File
NIM.....Network Interface Module
PED.....Parameter Entry Display
PI.....Personality Image
PLC.....Programmable Logic Controller
PM.....Process Module
PMM.....Process Manager Module
PSD.....Power Supply Distribution Module
PSU.....Power Supply Unit
PU.....Processing Unit
RAM.....Random Access Memory
ROM.....Read-Only Memory
SM.....Safety Manager
SOE.....Sequence of Events
TAC.....Technical Assistance Center
TDC.....Total Distributed Control
TDF.....Translated Database File
TPS.....TotalPlant Solution
UCN.....Universal Control Network
US.....Universal Station
VBD.....Vertical Bus Driver
WD.....Watchdog

Parameters

References

For TPS documentation:

Publication Title	Publication Number	Binder Title	Binder Number
FSC Safety Manager Control Functions	FS09-500	Implementation FSC Safety Manager	TPS 3076
FSC Safety Manager Installation Guide	FS20-500	Implementation FSC Safety Manager	TPS 3076
FSC Safety Manager Parameter Reference Dictionary	FS09-550	Implementation FSC Safety Manager	TPS 3076
FSC Safety Manager Configuration Forms	FS88-500	Implementation FSC Safety Manager	TPS 3076
FSC Safety Manager Service Manual	FS13-500	Implementation FSC Safety Manager	TPS 3076

For FSC documentation:

Publication Title	Publication Number	Version
FSC Safety Manual	PM.MAN.8047	400
FSC Hardware Manual	PM.MAN.8048	400
FSC Software Manual	PM.MAN.8025	400

Section 1 – Introduction

1.1 Implementation Overview

Section summary

This section contains the following topics:

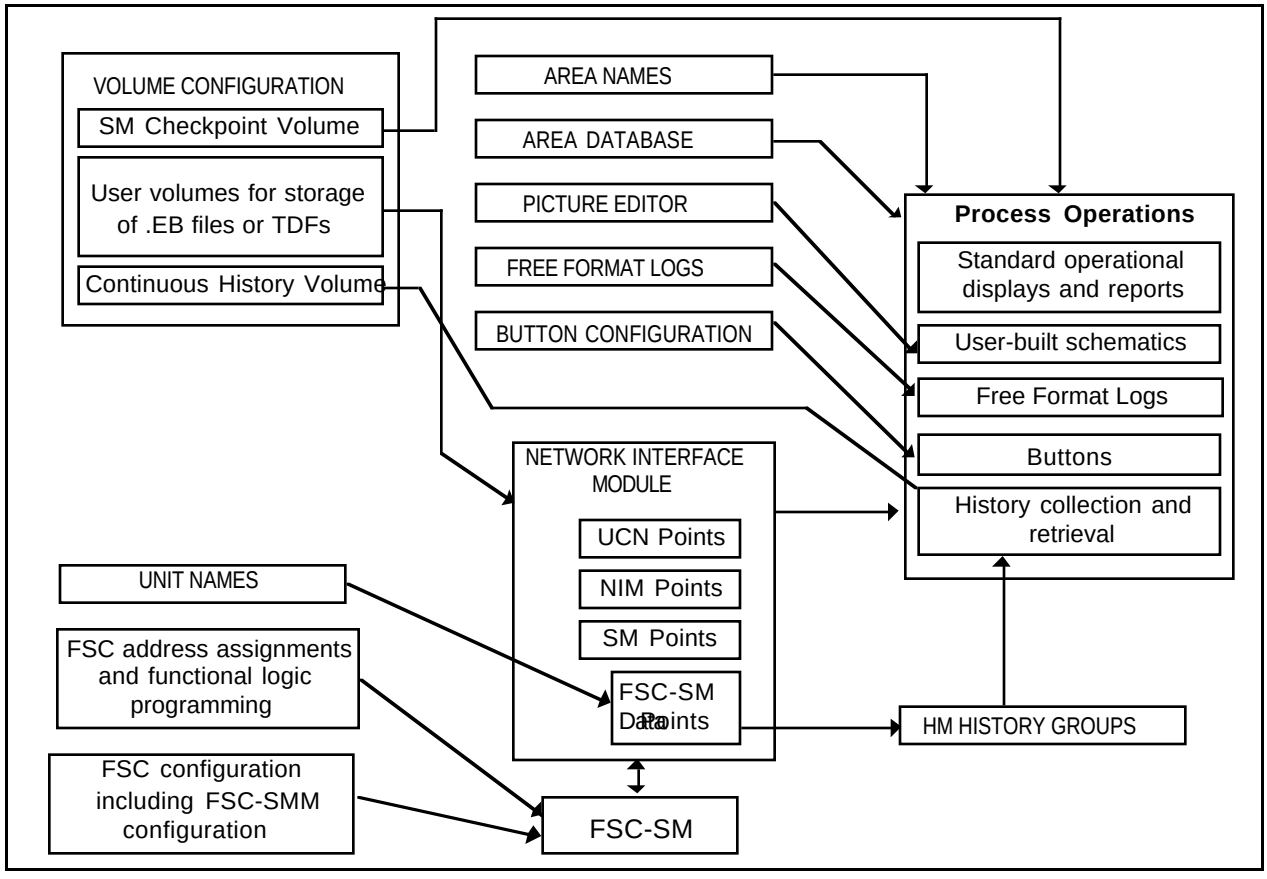
Summary of FSC-SM implementation tasks

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

FSC-SM implementation dependencies

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

Figure 1-1 – FSC Safety Manager Implementation Dependencies



FSC-SM implementation tasks

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

Table 1-1 – Factors Affecting FSC-SM Implementation Tasks

Item	Description
Unit Names	The process units are defined for each FSC-SM data point.
Area Names	The area name and descriptor are defined for any units with FSC-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 FSC-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 FSC-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 FSC-SM points are built in this activity.
Network Interface Module	UCN points which define to the UCN where an FSC-SM resides, and the node-specific points that define the nodes on that UCN, including the NIM and the FSC-SM, are built in this activity. Also, FSC-SM data points are built in this activity. Connections to the FSC-SM points are defined in `tagname.parameter` form. **ATTENTION** Prior to point building, the FSC-SMM must be configured on the FSC. FSC addresses must also be defined.
Picture Editor, Free Format Logs, Button Configuration	Any pictures, logs and buttons built by these activities can access FSC-SM points once the points are built and loaded.
HM History Groups	FSC-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 Database	This activity defines how and where data for data points, including FSC-SM data points, are used and displayed in a given process area. The area database is the database loaded into a Universal Station (US), and thus defines the process area monitored and controlled through the US.
Control Language (CL)	CL/AM and CL/PM programs can access FSC-SM parameter values. CL/CM programs cannot access FSC-SM parameter values. A Control Language that runs on an FSC-SM is not available.
Functional Logic Programming	This is accomplished through the FSC Development System (FSC-DS) which is connected to an FSC Communication Module. The FSC-DS provides an interface and software which are installed in a DOS-based IBM-compatible personal computer.

1.2 FSC Safety Manager Functional Summary

FSC Safety Manager summary

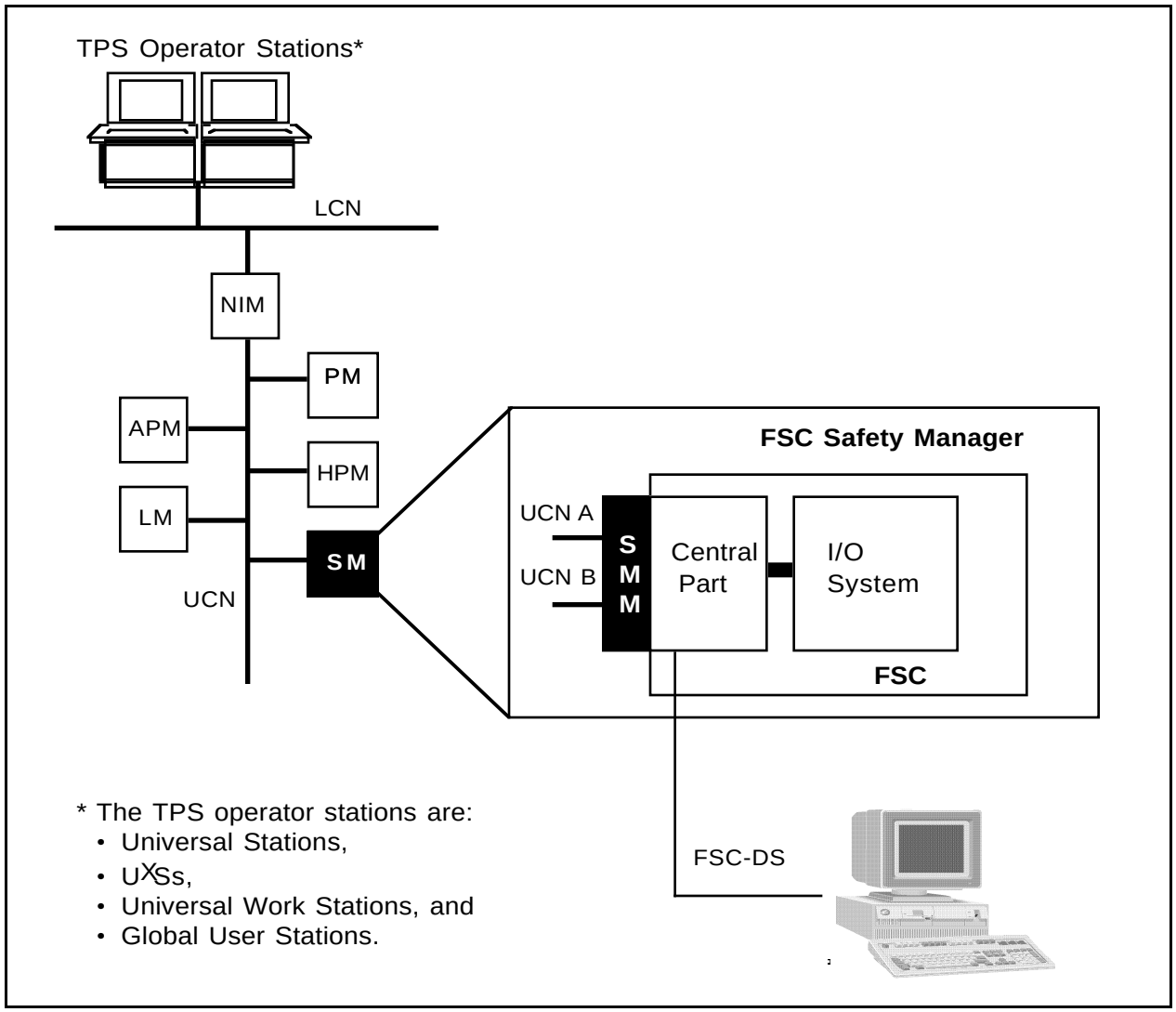
The FSC Safety Manager (FSC-SM) provides a dual redundant fault-tolerant controller for safety and shutdown application on the Universal Control Network (UCN).

The FSC-SM consists of an FSC controller and an FSC Safety Manager Module (FSC-SMM). The FSC-SMM provides the interface to the UCN.

FSC Safety Manager diagram

Figure 1-2 gives an overview of the FSC Safety Manager connected to the TotalPlant Solution (TPS) network.

Figure 1-2 – FSC Safety Manager Relationship to the TPS system



Continued on next page

Functional overview

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

- FSC Safety Manager Module
- FSC controller — including these components:
  - Control Processors,
  - Communication Modules,
  - I/O Modules,
  - Power Supply Modules,

FSC-SMM functions

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

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

FSC Control Processor functions

The FSC Control Processors execute the control program as defined by the user in the Functional Logic Diagrams (FLDs).

The Control Processors read and synchronize the inputs. The inputs are then processed by the control program and the result is updated to the output modules.

The FSC Control Processors perform self-tests of the FSC hardware on a continuous basis. Diagnostic information on detected faults is provided to the FSC-SMM for reporting at the US.

FSC Development System functions

Via the FSC-DS at the FSC level of the FSC Safety Manager, the user:

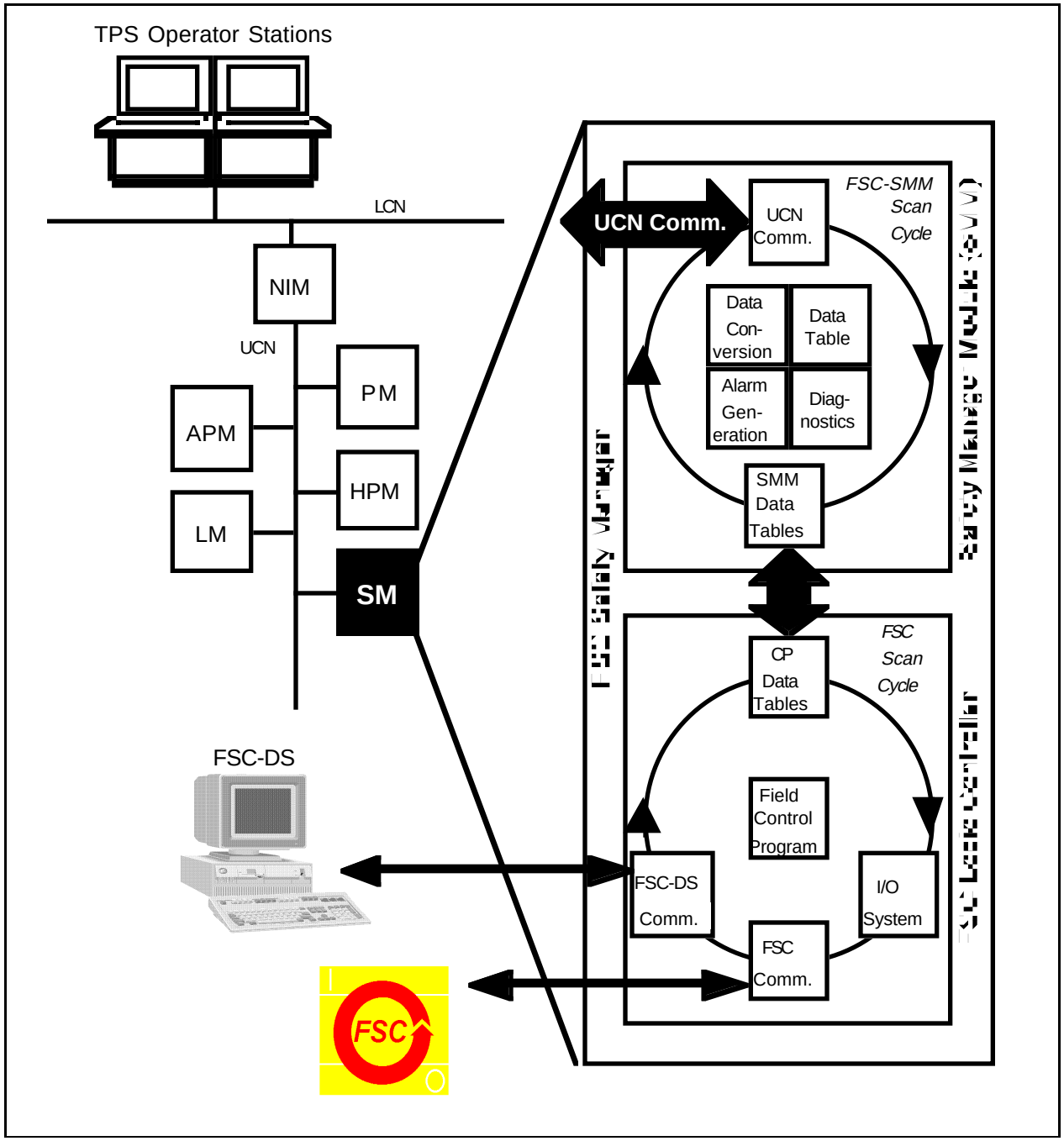
- configures FSC variables and attributes,
- creates the control program via Functional Logic Diagrams,
- loads the control program into the FSC-SM,
- monitors the system status, and
- forces FSC variables for loop check-out and maintenance of field devices.

Continued on next page

FSC Safety Manager functional diagram

Figure 1-3 illustrates the FSC Safety Manager subsystem.

Figure 1-3 – FSC Safety Manager Conceptual Diagram



1.3 FSC Safety Manager Data Flow

UCN to field and back

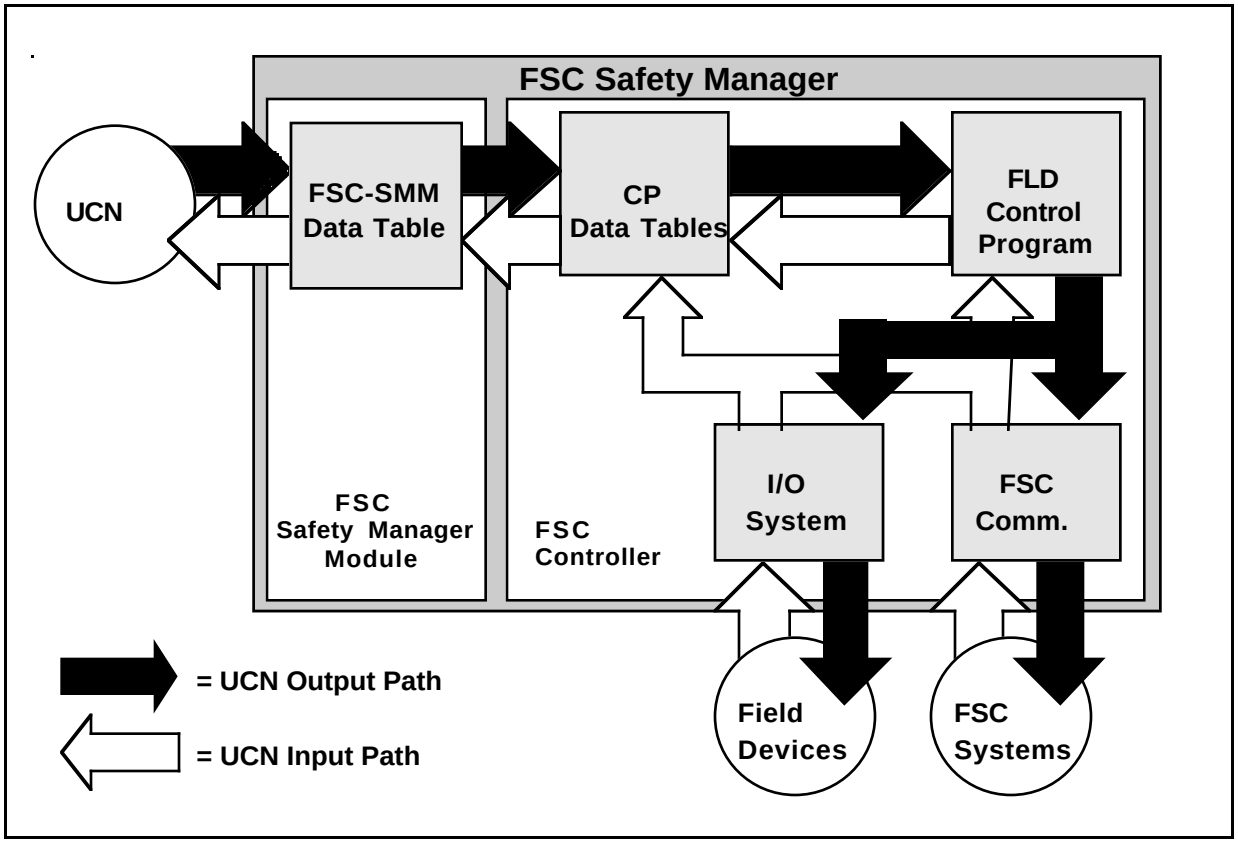
As illustrated in Figure 1-4, data being written to, and read from, the I/O system takes two paths within the FSC Safety Manager.

- The UCN output path:
  - receives data from the UCN,
  - posts the data in the FSC-SMM's Data Table,
  - transfers the data to the Control Processor's Data Tables,
  - processes (tests, modifies) the data in the FLD control program,
  - posts the processed data back to the Control Processor's Data Table, and
  - sends the processed data to the field via the I/O system or
  - sends to other FSC systems via the FSC Communication Network.
- The UCN input path:
  - collects data directly from the field via the I/O system or via the FLD control program, or
  - collects data from other FSC systems via the FSC Communication Network, and
  - posts the data in the Control Processor's Data Tables,
  - transfers the processed data to the FSC-SMM's Data Table, and
  - places the data on the UCN.

ATTENTION The FLD control program running in the FSC is in the path between the FSC-SMM output data points and the I/O subsystem. The FLD 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 FLD control program is doing, as it is not possible to view the FLD control program from the US.

Continued on next page

Figure 1-4 – Data Flow: UCN to Field and Back



Left blank intentionally

Section 2 – FSC-SM Operational Considerations

2.1 FSC Safety Manager Operating Modes

Section summary

This section contains the following topics:

FSC-SM operating and startup modes

The FSC Safety Manager supports two basic operating modes: RUN mode and RAM mode. For each of the basic operating modes, two startup modes are supported.
The operating modes apply to the type of physical memory the FSC Control Program is located in. The startup modes apply to the process control behavior of the FSC Control Processors when started after being shutdown.

The FSC-SM operating and startup modes are defined during configuration of FSC, at the FSC Development System.

RUN mode

When the FSC-SM is configured for RUN mode, the FSC Control Program is located in EPROM.

EPROMs are programmed at the dedicated FSC EPROM Programmer using the FSC Development System option ‘Program application in EPROMs’. The EPROMs are placed at the memory module of the FSC Central Processing Unit (CPU) hardware module.

RAM mode

When the FSC-SM is configured for RAM mode, the FSC Control Program is located in RAM.

The FSC Control Program is loaded in the RAM of the FSC Control Processor via a serial communication link using the FSC Development System option ‘View FSC system and process status’.

ATTENTION RAM mode only applies to the part of FSC Control Program located at the FSC CPU module. The part of the FSC Control Program for the FSC Communication Processors is always located in EPROM.

Coldstart

When the FSC-SM startup mode is Coldstart, the FSC Control Processor initializes all variables to the configured power-on values before processing the FLD Control Program for the first time after startup.

Power-up values for FSC variables are configured with the process interfaces definitions using the FSC Development System option 'Configure FSC System'.

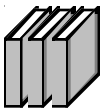
Warmstart

When the FSC-SM startup mode is Warmstart, after startup, the FSC Control Processor resumes execution of the FLD Control Program, using the variable status as it existed at the moment of the shutdown of the Control Processor.

When the FSC Control Processor is started for the first time after download of a new Control Program in RAM, or if the Control Processor was shut down because of a detected safety-critical hardware fault, the Control Processor starts up as with the Coldstart mode, initializing all variables to the configured power-on values before processing the FLD Control Program for the first time.

ATTENTION For FSC-SM configurations with redundant Control Processors, the startup mode only applies if both Control Processors were shut down. If a Control Processor is started while the redundant Control Processor is running, the starting Control Processor is synchronized to the current processing status before it starts processing the FSC Control Program for the first time.

ATTENTION In FSC-SM configurations configured for Warmstart, the FSC Control Processor that was shut down last should always be started first, as the status of this Control Processor best resembles the actual operational state of the process.



Refer to the *FSC Hardware Manual* and *FSC Software Manual* for further details.

Continued on next page

FSC Configuration and FLD Control Program Design

The safety functions of the FSC-SM and the actual process interface is realized through the FSC part of the FSC Safety Manager. The FSC configuration and the design of the Control Program, by means of Functional Logic Diagrams, is accomplished through the options of the FSC Development System.
Table 2-1 lists the FSC Development System options of interest for configuration and FLD design for the FSC part of the FSC-SM.

Table 2-1 – FSC Development System Options

FSC-DS Option	Description
Configure FSC system	A configuration tool to: • define the FSC hardware configuration (including the FSC-SMM), • define the interface of the FSC system to the process, • define the alias addresses to link FSC variables to FSC-SMM points, • define the interface to devices and other FSC systems via serial communication links.
Print FSC system configuration	Print a hardcopy of the engineering documentation as defined via the 'Configure FSC system' option
Design functional logic diagrams	A graphical tool to define the FSC Control Program in Functional Logic Diagrams containing Arithmetic, Logic and Timing functional symbols.
Hardcopy of functional logic diagrams	Print a hardcopy of the Functional Logic Diagrams as designed via the 'Design functional logic diagrams' option.
Translate application	A tool to: • verify the correct and consistent implementation of the FSC Configuration and the Functional Logic Diagrams, • convert the FSC Configuration Database and Functional Logic Diagrams into a format which can be executed by the FSC Control Processor.
Show application logging files	View the results of other FSC-DS options, e.g. 'Translate FSC application' and 'Verify application in FSC system'.
Program application in EPROMs	Program EPROMs for the FSC Control and Communication Processors.

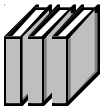
Continued on next page

FSC Configuration and FLD Control Program Design, continued

Table 2-1 – FSC Development System Options (continued)

FSC-DS Option	Description
Verify application in FSC system	A tool which communicates with the FSC system to: • verify the correct translation and download of the FSC Configuration and Functional Logic Diagrams, • log changes made to the FSC configuration and Functional Logic Diagrams.
View FSC system and process status	A tool which communicates with the FSC system to: • load the FSC Control Program into the RAM of the FSC Control Processor, • monitor process signals on a per-signal basis, e.g. for loop checking, • monitor the Control Program status per Functional Logic Diagram, • retrieve FSC system and field loop diagnostic information from the FSC system.

ATTENTION The Functional Logic Diagrams and Alias Address assignments within the FSC cannot be modified from the US, LCN or UCN levels.



For further details on FSC configuration and the design of Functional Logic Diagrams, refer to the *FSC Software Manual.*

2.2 Address Aliases

DCS address

FSC-SM points are linked to FSC variables via alias addresses.

For FSC variables, the alias address is referred to as the DCS address. A DCS address is a five-digit number assigned to a variable in the FSC that allows nodes on the UCN to reference that variable. The DCS address of an FSC variable is the counterpart of the PLC address of an FSC-SM point.

FSC variable access rights

Table 2-2 lists the valid combinations of FSC-SM points and FSC variables and access rights for the FSC Safety Manager Module (FSC-SMM).

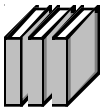
Table 2-2 – FSC-SM - FSC Variable Combinations and FSC-SMM Access Rights

FSC-SM point	FSC variable	FSC-SMM Access Rights	Note
Analog Input (AI)	Analog Input (AI)	Read Only	
	Analog Output (AO)	Read Only	
	Numerical Input (BI)	Read Only	1,2
	Numerical Output (BO)	Read Only	1,2
Analog Output (AO)	Numerical Input (BI)	Write Only	1,2,3
Digital Input (DI)	Digital Input (I)	Read Only	
	Digital Output (O)	Read Only	
Digital Output (DO)	Digital Input	Write Only	
Digital Composite (DC)	Digital Input (I)	Read/Write	3
	Digital Output (O)	Read Only	
Numeric (N)	Numerical Input (BI)	Read/Write	3
Logic (L)	Analog Input (AI)	Read Only	
	Analog Output (AO)	Read Only	
	Digital Input (I)	Read/Write	3
	Digital Output (O)	Read Only	
	Numerical Input (BI)	Read/Write	3
	Numerical Output (BO)	Read Only	
Flag (F)	Digital Input (I)	Read/Write	3
Timer (T)			
PV	Timer (T)	Read Only	
Start	Digital Input (I)	Write Only	3
Reset	Digital Input (I)	Write Only	3
Setpoint	Numerical Input (BI)	Write Only	3

Continued on next page

FSC variable access rights, continued

Notes:
1. The format of FSC BI and BO variables must be Float.
2. The value for FSC BI and BO variables linked to FSC-SM Analog Input and Output points is restricted to integer numbers in the range 0..4095.
3. To assure the integrity of the safety critical function of the FSC part of the FSC-SM, the FSC-SMM has no direct write access to outputs of the FSC system. All write access is routed through FSC input variables (I, BI) with location COM. Via the FLD Control Program, the condition for output control is realized.



For more information refer to Section 2.4 of the *FSC Safety Manager Control Functions* manual.

Linking FSC-SMM points to FSC variables

A link between an FSC-SMM point and an FSC variable is made when the combination of the FSC-SMM point type and FSC variable is valid and the FSC-SMM point PLC address matches the FSC variable DCS address.

Assigning Alias Addresses

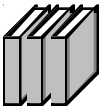
DCS addresses are assigned to FSC variables on an individual basis, using the FSC-DS option 'Configure FSC System'.

The following rules apply:

- The FSC variables type I with location COM are grouped in areas. The FSC Control Processor references these variables by their relative address in their area. If the FSC variable I is linked to an FSC-SMM Flag point, the DCS address of the first I variable (and PLC address of the link Flag point) can be selected freely. All subsequent I variables and Flag points must be assigned the DCS/PLC address of the first variable/point, plus the difference between the relative FSC address of the variable with respect to the starting I variable.
- If a Flag point is linked to an FSC variable of type I, location COM, with relative address 5, and the DCS address is set at 1000, then the DCS address for the I variable with relative address 20 must be 1015.
- For the FSC variable type BI, location COM, linked to an FSC-SMM Numeric point, the same rule for DCS address assignment applies as described above for FSC variable type I, location COM, linked to an FSC-SMM Flag point.

Assigning Alias Addresses, continued

- Although the FSC variable types O and BO are also grouped in areas, this rule for DCS address assignment does not apply to the O and BO variables.
- For an FSC-SMM Timer point, four DCS addresses must be assigned. The DCS address for the PV, Setpoint and Set parameters of the Timer point can be selected freely. The DCS address for the Reset parameter must match the DCS address of the Set parameter plus 1.



For more information on DCS address assignment to FSC variables, refer to the *FSC Software Manual.*

2.3 I/O System

I/O system

The interconnection of the FSC-SM with the process is realized through I/O modules located in the FSC part of the FSC-SM.
I/O modules can be located in the FSC Central Part rack, or in I/O racks.
The interconnection between the Control Processor and the I/O system is realized via Vertical Busses.
In FSC-SM configurations with redundant Control Processors, the I/O system can be redundant, non-redundant, or a combination of both. In the latter case, Independent Vertical Busses are used to control the I/O system.

Non-Redundant I/O

In configurations with non-redundant I/O, 18 I/O modules can be located in a single I/O rack. The modules in the non-redundant I/O section are controlled by the first Control Processor and the second Control Processor alternately.

In configurations which combine redundant I/O and non-redundant I/O, an independent Vertical Bus is used to interconnect the both Control Processors in parallel with the non-redundant I/O modules.

Redundant I/O

In configurations with redundant I/O, 9 I/O module pairs can be located in a single I/O rack. For each pair, one I/O module is controlled by the first Control Processor the other I/O module is controlled by the second Control Processor.

The I/O signals of the redundant pairs are wired in parallel to the field.

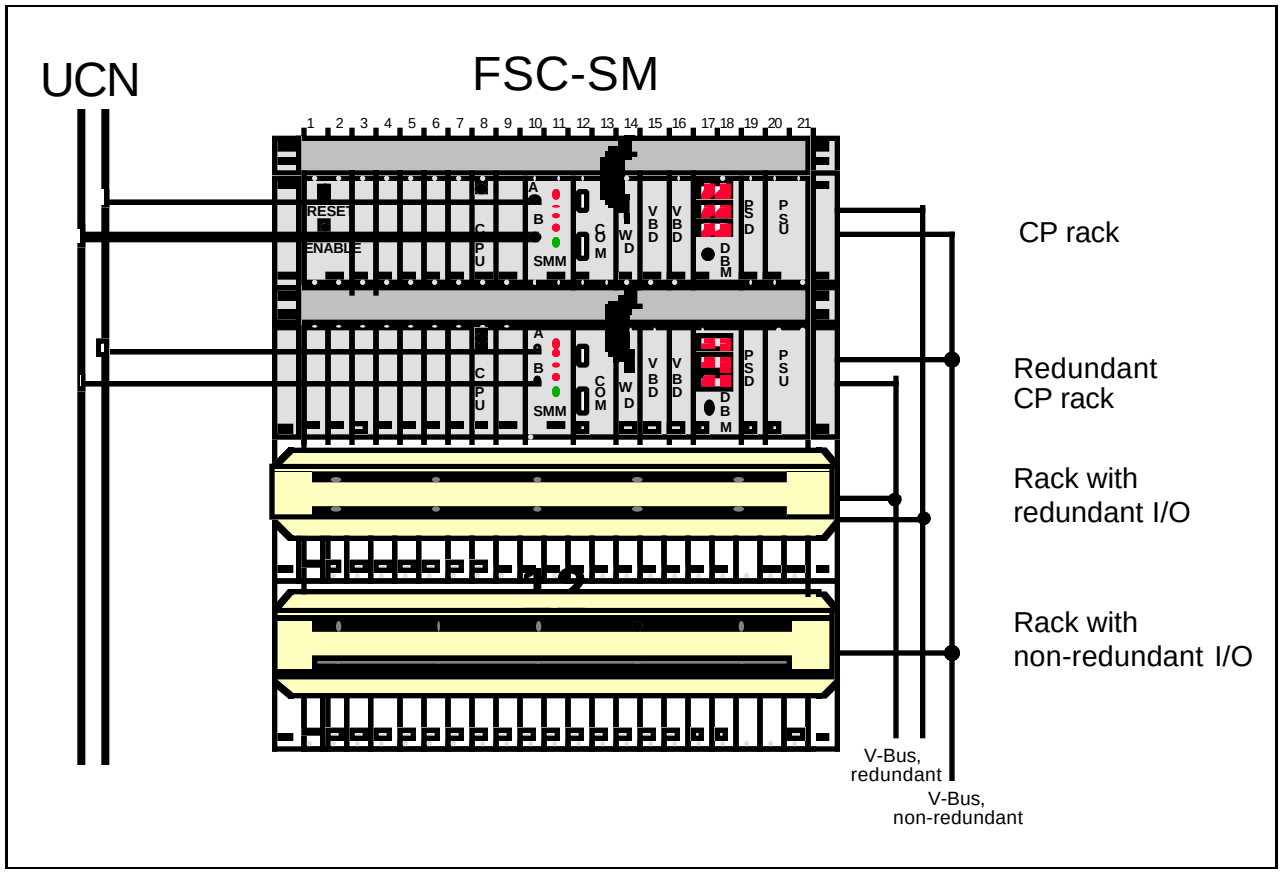
Separate Vertical Busses interconnect the Control Processors with their own I/O modules.

Continued on next page

I/O System diagram

Figure 2-1 is an example diagram of the FSC-SM I/O system configurations.

Figure 2-1 – Local and Remote I/O Subsystem Configuration Example



I/O types supported

The FSC Safety Manager supports digital and analog input and output signals.
The I/O signals can be terminated in the FSC cabinet, at ELCO or Terminal Field Termination Assemblies, or can be terminated externally, e.g. in marshaling cabinets.

Continued on next page

I/O characteristics

Table 2-3 describes the associated I/O characteristics with the various module types.

Table 2-3 – I/O Characteristics for the Various Module Types

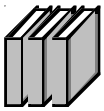
Field Inputs		Field Outputs	
• Digital	24, 48, 60 VDC	• Digital	24, 48, 60, 110, 220 VDC
	115 VAC	• Digital	115 VAC
• Analog	0(4) - 20 mA	• Analog	0(4) - 20 mA
	0(1) - 5 VDC	• Relay	
	0(2) - 10 VDC		

2.4 FSC Networks

FSC network capabilities

FSC systems can be interconnected in communication networks.

The network is realized through serial communication links, dedicated for data exchange between the FSC systems.
Data exchange is based on the Honeywell Safety Management Systems proprietary FSC Communication Protocol, which allows exchange of safety critical information.



For more information regarding the FSC networking capabilities, refer to the *FSC Safety Manual* and *FSC Software Manual.*

2.5 Sequence of Events (SOE)

SOE summary

During each program scan, the FSC's Control Processor (CP) updates its data tables to the FSC-SMM, including timestamp information when the data was read from/updated to the field*.
The FSC-SMM processor examines designated discrete variables, linked to FSC-SMM digital input (DI) points, for a change of state (an event). When the FSC-SMM processor detects an event for a DI point which was configured for SOE, it generates an event, using the FSC timestamp for event processing.

* Timestamps applied by the FSC are on a "per scan" basis.

FSC-SM SOE configuration

SOE within FSC-SM involves user configuration of the FSC-SMM for:

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

Time synchronization

Time synchronization is transparent to the user and has the following characteristics:

- The NIM provides time synchronization for all nodes on the UCN.
- The FSC-SMM synchronizes the clock on the FSC Control Processors to LCN time - having a clock resolution of 1 millisecond.

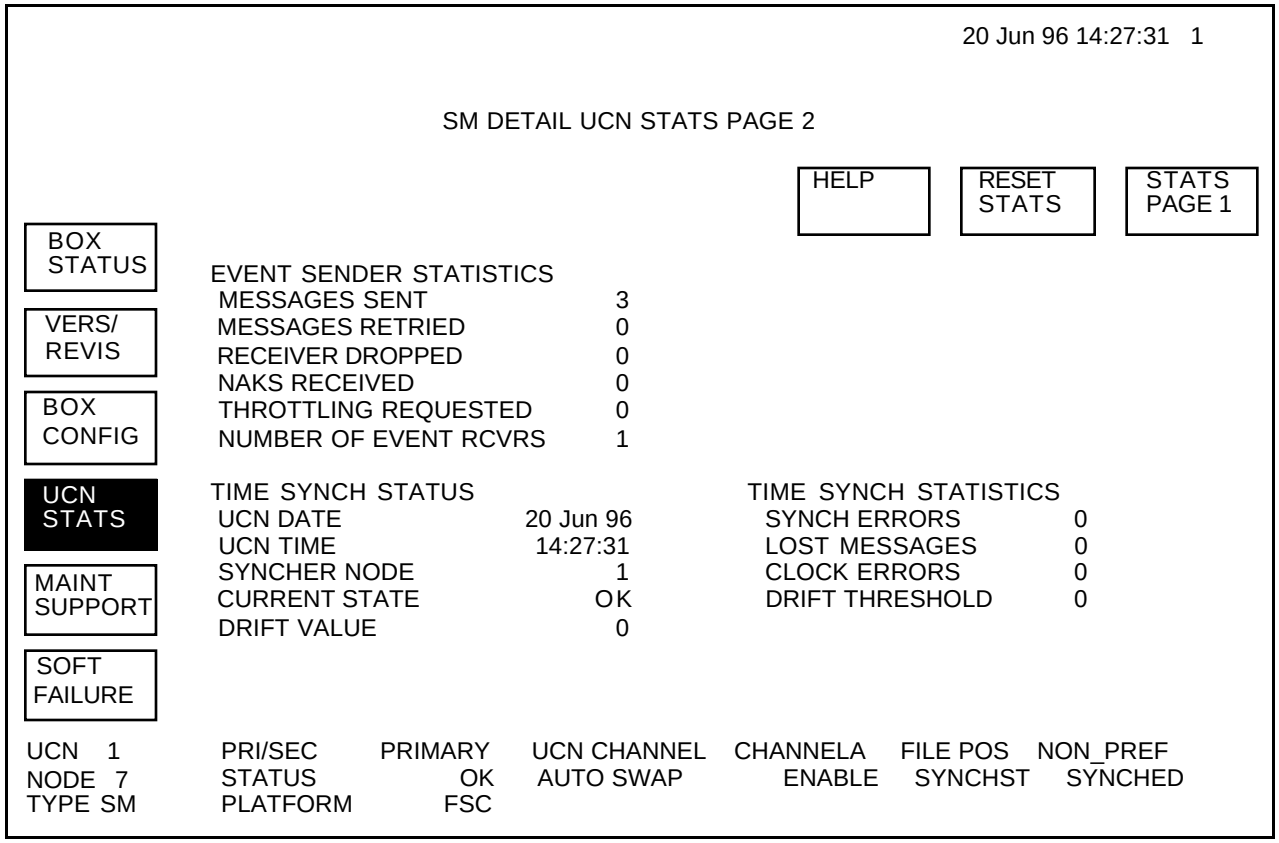
ATTENTION The FSC-SM Time Sync will override any attempt by the user to set FSC time using the FSC Development System.

Continued on next page

Time Sync diagram

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

Figure 2-2 – Diagnostics Display UCN Statistics: Time Sync Parameters



Continued on next page

Comparing events between FSCs

The NIM and FSC-SM have time synchronization features which keep time within all the FSC-SMs within ±3 ms.

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

Timestamping within the FSC

Timestamps within the FSC have the following characteristics:

- Timestamps are based on FSC clock time measured and synchronized between the FSC Control Processors following the refresh of the Input Status.
- All detected events within a given FSC scan will have a timestamp of the same value of time.
- After each FSC Control Program cycle, the FSC Control Processor updates its data tables, including timestamp information, to the FSC-SMM.
- The FSC-SMM monitors the DI data table for all DI points configured for SOE, and generates an SOE event if a state change is detected. The timestamp used for the SOE event is the timestamp provided by the FSC Control Processor.

DI SOE timestamping

The FSC-SM clock is synchronized to the LCN time provided through the NIM for consistent and comparable timestamping of DI SOE events throughout the TotalPlant Solution (TPS) system.

Timestamping for the FSC-SM is the responsibility of the FSC-SMM Processors. The FSC-SMM collects any DI events once per FSC Control Program cycle and uses the same clock time to timestamp all events within that cycle.

Non-DI SOE event/alarm timestamping

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

SOE resolution

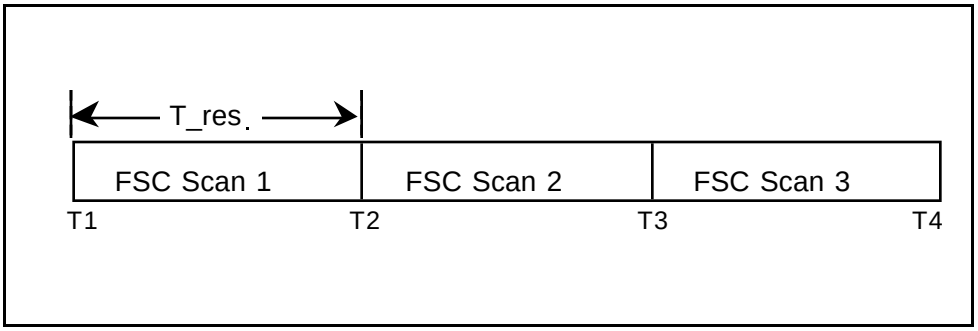
SOE resolution (T_res) is equivalent to the FSC Control Program Cycle Time. This cycle time is calculated by the FSC-DS depending on the FSC configuration and Control Program.

Continued on next page

SOE resolution diagram

Figure 2-3 illustrates SOE resolution (T_res) for the FSC.

Figure 2-3 – SOE Resolution



SOE event recovery

Event recovery of timestamped events is characterized by the following:

- Occurs only during FSC-SMM or NIM failover/switchover.
- No operator intervention is required.
- The FSC-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 no more than 20 seconds old.
- During buffer overflow situations (no available buffer space and no events older than 20 seconds), the FSC-SM will drop new events.

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

SOE event recovery cut-off point

SOE Event Recovery ends when:

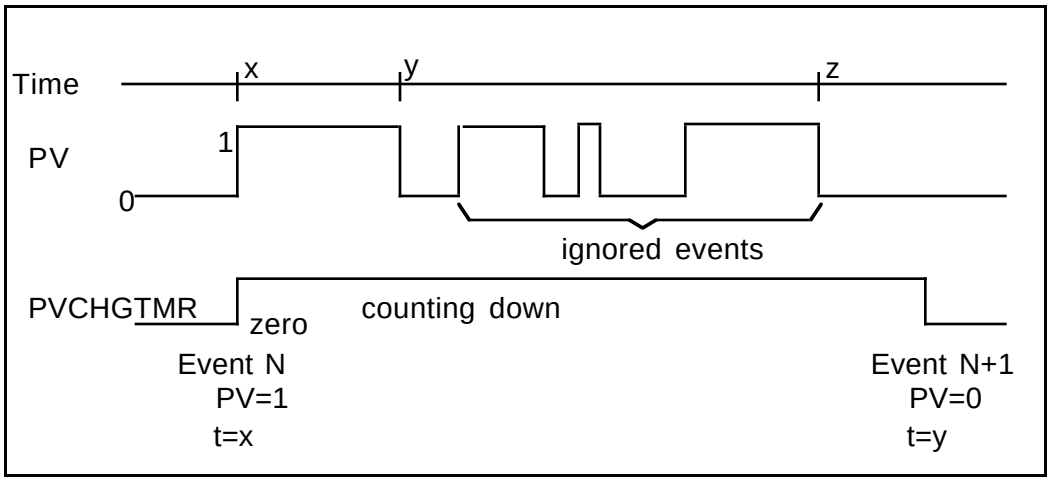
- event timestamps exceed the LCN time at start of recovery and
- the FSC SOE Event Buffer is emptied.

Continued on next page

Throttled event collection

FSC-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 2-4 illustrates how unwanted changes in events are ignored.

Figure 2-4 – Throttled Event Collection



Event recovery and flushing

Flushing an FSC-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.
- FSC-SMM will distribute timestamped events per established UCN procedures.
- Total local alarm and event output is limited to 512 over any 10 second period.
- Long-term SOE may not exceed 16 events per second.

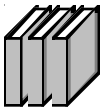
Continued on next page

Journals and listings	Displayed timestamp resolution will be to 1 ms, with Sequence Stamp Differences equivalent to FSC Scan Time.
SOE configuration	To use SOE, you must configure the selected DI points to be collected for SOE on the TPS system.

2.6 Saving and Restoring FSC Safety Manager Data

Restoring and saving data summary

Checkpoint saving/restoring and saving/restoring Functional Logic Diagram (FLD) control programs are separate operations. FLD control programs are saved and restored in the FSC-SM using the FSC-DS. Checkpoint saving and restoring is done at the US.

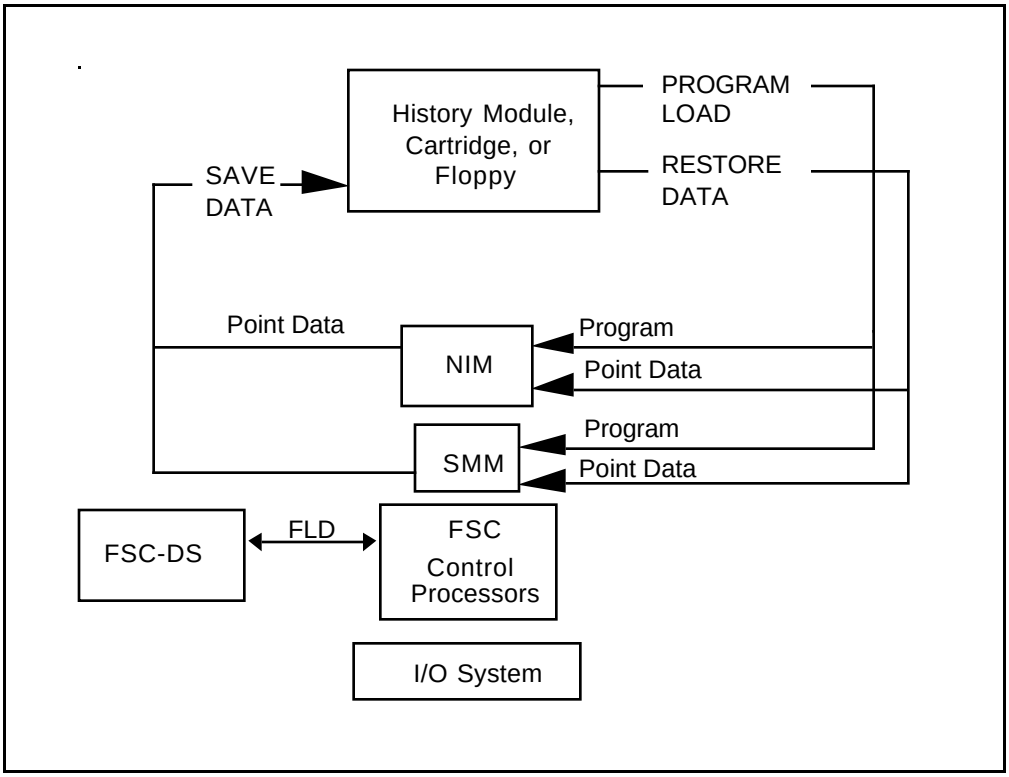


For more information refer to the *FSC Software Manual.*

Saving/restoring data flow

Figure 2-5 shows the saving and restoring data flow for the FSC Safety Manager.

Figure 2-5 – FSC-SM Saving and Restoring Data Flow

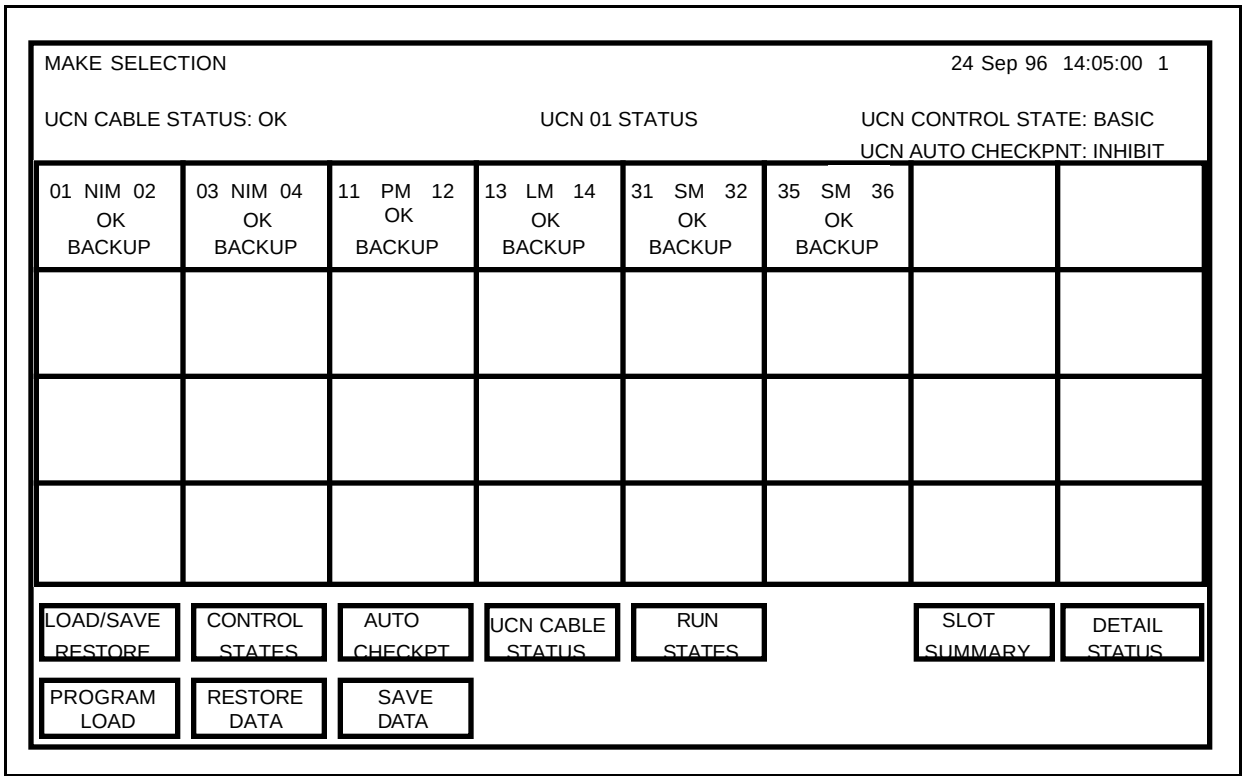


Continued on next page

Saving and restoring data using the US Status display

The three bottom targets of the UCN Status display, shown in Figure 2-6, save and restore the NIM and FSC Safety Manager data points.

Figure 2-6 – US UCN Status Display for Data Save and Restore



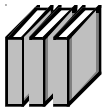
Continued on next page

Function of save and restore targets

Table 2-4 outlines the functions of the US Status display save/restore targets.

Table 2-4 – Save and Restore Command Functions

Command	Description
PROGRAM LOAD	Loads the NIM and FSC-SMM software personality image from the &UCN volume on an HM, or from a cartridge or floppy, to the NIM and selected FSC-SMM(s) in the selected FSC 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 FSC-SMM(s) in the selected FSC Safety Manager(s).
SAVE DATA	Saves point data in the NIM and FSC-SMM(s) in the selected FSC 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.

Section 3 – Redundant FSC Safety Managers

3.1 Redundancy Overview

Section summary

This section contains the following topics:

Overview

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

- FSC - Dual Channel Redundant configuration.
- FSC-SMM - hot spare module in the redundant FSC Central Part.

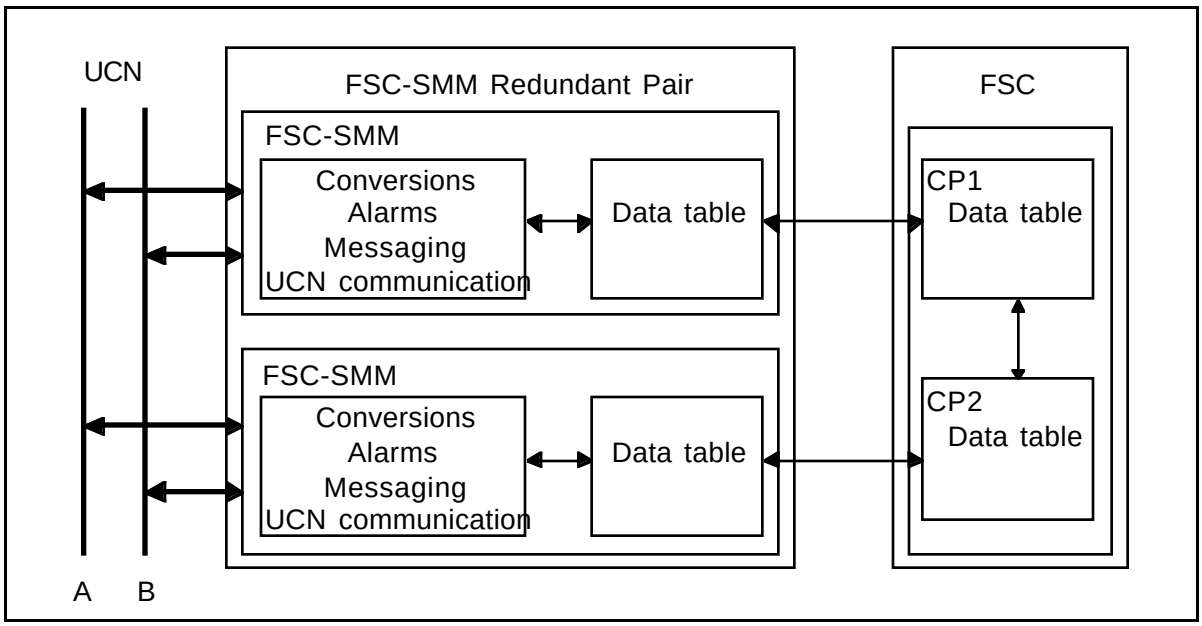
This subsection will focus primarily on the FSC Safety Manager FSC-SMM redundancy.

ATTENTION FSC-SMM redundancy does not interfere with FSC redundancy. If, however, a failure is detected by an FSC Control Processor which requires the processor to shut down, the state of the associated FSC-SMM will be affected.

FSC-SMM /FSC redundancy scheme

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

Figure 3-1 – Redundant FSC Safety Manager Connected to the UCN and FSC



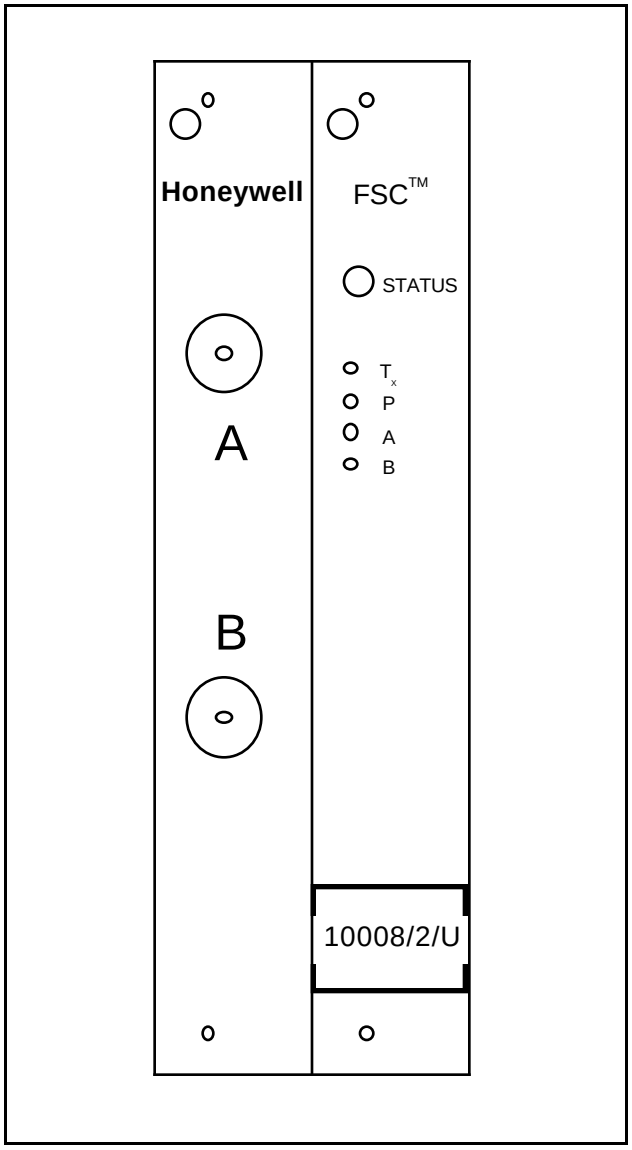
FSC Safety Manager status indication

Both FSC-SMMs communicate with the UCN, but only the Primary performs main functions like point processing, etc. The other FSC-SMM, the Secondary, is in hot stand-by.

The status of the FSC-SMM is shown on the front panel of the module.

Figure 3-2 shows the front panel of an FSC Safety Manager Module.

Figure 3-2 – FSC Safety Manager front panel



Continued on next page

FSC-SMM front panel indications

The STATUS, Tx, P and the A and B LED indicators, as seen in Figure 3-2, provide information on the status of the FSC-SMM. Table 3-1 gives an overview of the description of each.

Table 3-1 – FSC-SMM Front Panel Indications

LED indicator	Description and Action
STATUS	GREEN – Personality Image is loaded and running. RED – Module is performing power-up self-tests or has entered the ALIVE state. RED/GREEN (flashing) – Module has entered the FAIL state.
Tx	When ON, the FSC-SMM is transmitting data to the UCN
P	ON – FSC-SMM is Primary OFF – FSC-SMM is Secondary
A, B	ON – preferred cable

FSC-SMM redundancy functional summary

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

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

Continued on next page

FSC-SMM and FSC redundancy interfacing

Each FSC-SMM monitors the link to its associated Control Processor. A fault in this interface will trigger the FSC-SMMs to choose the best of two FSC interface situations. Failure of a link to an FSC Control Processor will initiate a failover. While both Control Processors are running, the FSC-SMMs will attempt to isolate the emerging failures and maintain the most effective interface.

Redundant FSC-SMMs route switchover requests through the UCN, and via the FSC Control Processors 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 FSC module installation guidelines, as they pertain to redundant communication cards, must also be followed with redundant FSC-SMMs. FSC-SMM configuration is done using the FSC Development System.

FSC-SMM failover

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

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

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

FSC-SMM switchover

FSC-SMM switchovers result from an Operator Station command. For operator-requested switchovers, the FSC-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

FSC-SMM switchover procedure

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

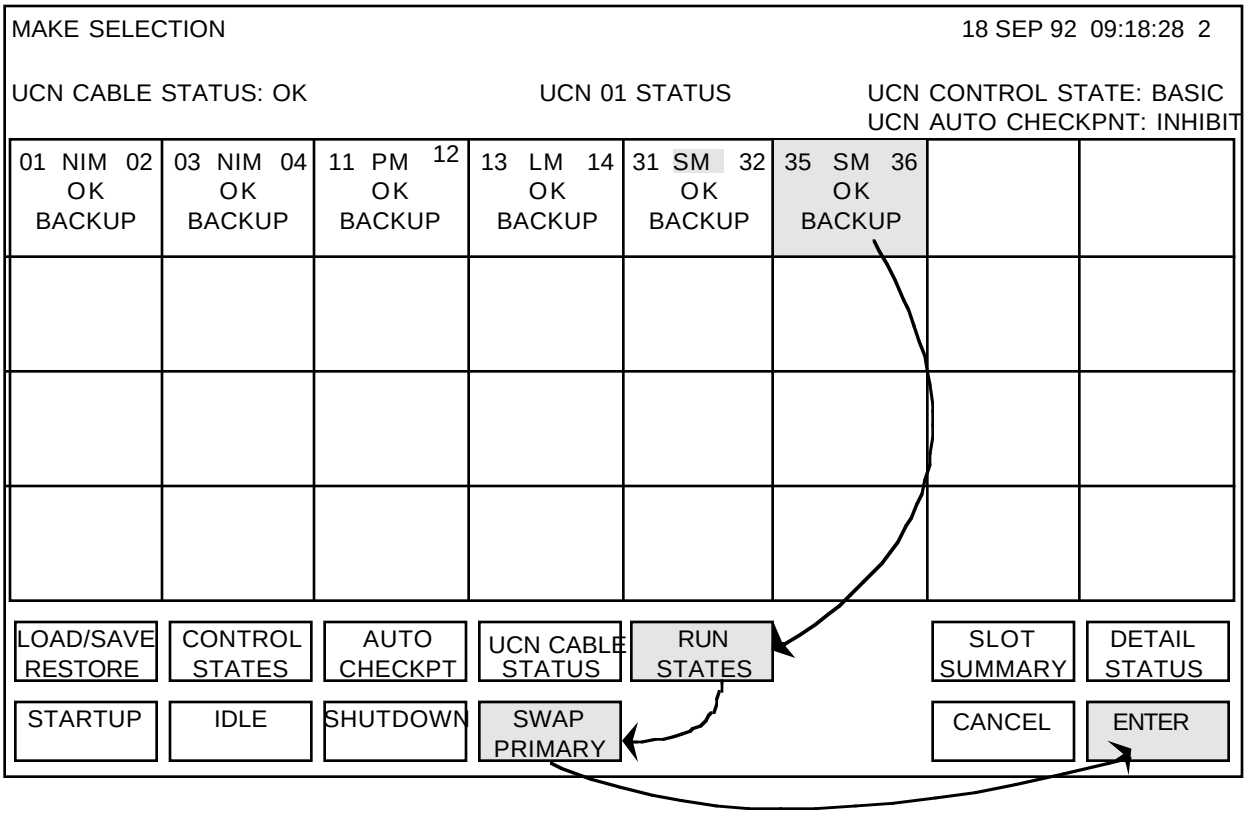
Table 3-2 – FSC-SMM Switchover Procedure

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

US UCN status display for FSC-SMM switchover

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

Figure 3-3 – US UCN Status Display for FSC-SMM Switchover



3.2 FSC-SMM Database Synchronization

FSC-SMM database synchronization

FSC-SMM database synchronization has the following characteristics:

- The FSC-SMM Primary will not automatically failover to an unsynced Secondary unless that Primary is unable to communicate over the UCN.
- Following operator requested switchovers, FSC-SMM database synchronization will occur in five seconds or less for a maximum 210 Kbyte database.
- If the Secondary is unsynced, the FSC-SMM will reject operator-initiated switchover requests.

FSC-SMM flushing

Flushing is the act of copying database changes between redundant pairs, and has the following characteristics:

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

Primary/secondary FSC-SMM UCN time sync

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

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

Continued on next page

FSC-SMM redundant communication paths

FSC-SMM redundant communication paths are characterized by the following:

- Functionally redundant communication operate on a continual basis.
- FSC-SMM initiates the switchover of FSC-SMMs via the FSC Control Processors by issuing requests to the FSC to set the FSC-SMM active or inactive.
- FSC-SMM uses the UCN to exchange data between redundant FSC-SMMs.
- FSC-SMM uses an intraslot (Primary to/from Secondary) messaging service provided by the FSC. This additional communications path assists the FSC-SMMs in diagnosing UCN or partner FSC-SMM problems.

UCN-specific FSC-SMM redundancy

UCN-specific FSC-SMM redundancy is characterized by the following:

- On-line and spare FSC-SMMs have unique addresses, allowing both to participate in UCN communications.
- Only the primary FSC-SMM in a pair can send point information on the UCN at any given time.
- The FSC-SMM uses the UCN to also exchange RDR (status) records between redundant FSC-SMMs.
- From the UCN's perspective, FSC-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 Node Addressing, UCN Status Display handling and redundancy status parameters.

ATTENTION If retries result in continued use of incorrect partner addressing, an FSC-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

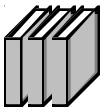
UCN addressing

The UCN address is configured via the FSC-DS and loaded with the control program into the FSC Control Processors. FSC-DS only allows odd UCN addresses to be configured.

In the ALIVE state, the FSC-SMM will display the odd address in the top slot or the even address in the bottom 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 FSC-SMM is installed, the FSC Control Processors load the UCN address into the FSC-SMM.



See the *FSC Software Manual* for configuration details.

Preference

Preference toward one of the FSC-SMMs enables the redundant pair to better resolve contention situations. Preference is based on top/bottom file position, the top is preferred (an FSC convention).

Hard failure

Hard failure situations will result in FSC-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 FSC Control Processor operation, but are considered detrimental to either the FSC, the partner FSC-SMM or the UCN.

ATTENTION The absence of communications will serve to signal the partner FSC-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.

Figure 3-4 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 3-4 – US UCN Status Display for a Failed Node

```
                                                        21 May 96 22:42:20   1


                SM DETAIL MAINT SUPPORT NODE STS INFO

                                          ERROR      NODE STS
                                          BLOCK        INFO
 BOX
 STATUS
                00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
 VERS/
 REV
                C0 08 01 30 24 34 01 30 00 00 00 00 00 00 04 0C
 BOX
 CONFIG
                00 00 20 08 00 50 0C C0 00 46 00 EA 00 46 00 EA
 UCN
 STATS          00 00 00 00 00 00 04 84 00 00
                ----D0-----  ----D1-----  ----D2-----  ----D3-----
 MAINT          00 5C DB 2C 00 00 00 05 00 00 00 5A 00 00 00 03
 SUPPORT        ----D4-----  ----D5-----  ----D6-----  ----D7-----
                00 00 00 00 00 00 00 00 00 00 45 00 00 00 00 0D
 SOFT           ----A0-----  ----A1-----  ----A2-----  ----A3-----
 FAILURE        00 5C DB 2C 00 5C DB 2C 00 00 00 00 00 4E 3D EC
                ----A4-----  ----A5-----  ----A6-----  ----A7-----
                00 5E 0E 34 01 30 24 00 00 59 B4 E0 00 5D 0C 6C

UCN    1      PRI/SEC    PRIMARY UCN CHANNEL  CHANNELB FILE POS NON_PREF
NODE  41      STATUS        FAIL AUTO SWAP      ENABLE SYNCHST   NOSYNCH
TYPE SM       PLATFORM       FSC
```

Left blank intentionally

Section 4 – FSC Safety Manager Start-up and Shutdown

4.1 Cold Start-up

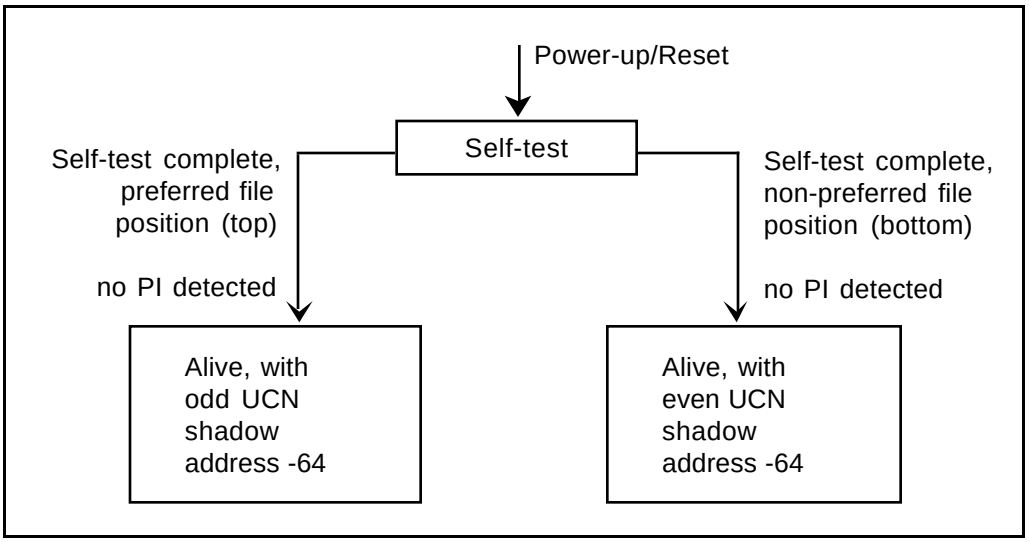
Section summary

This section contains the following topics:

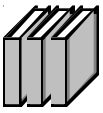
Cold start-up

Following power-up reset, the FSC-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 FSC-SMM can enter the ALIVE state, a Control Program with the FSC-SMM configured must have been previously loaded by the FSC-DS into the FSC.



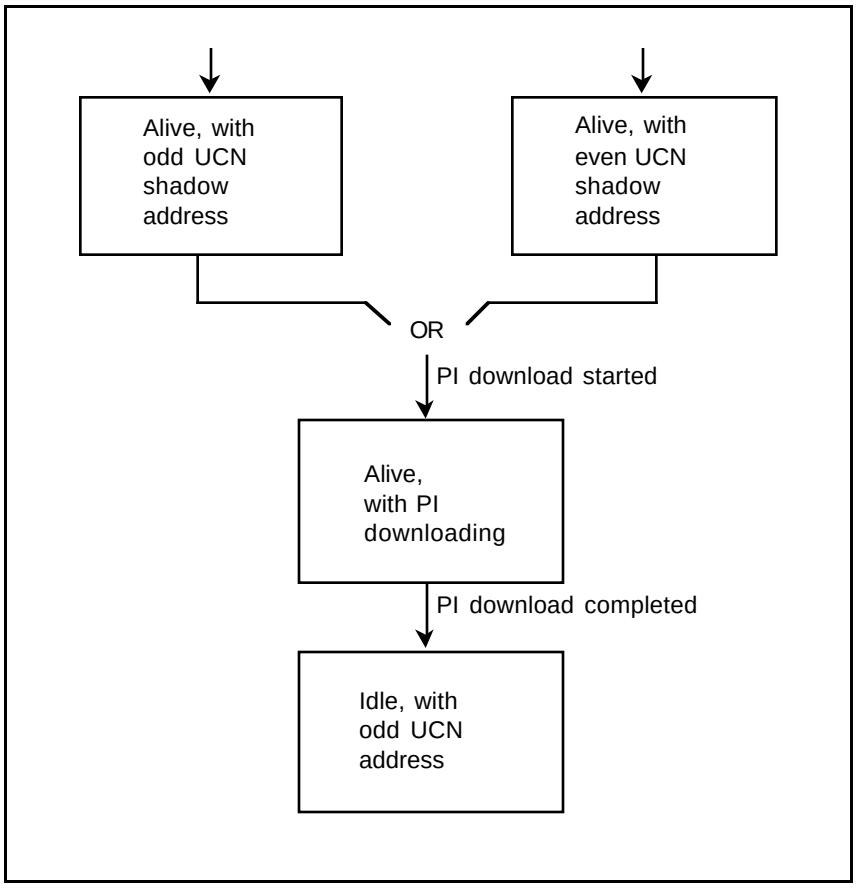
For more information on FSC start-up and shutdown, refer to the *FSC Software Manual.*

Continued on next page

Downloading FSC-SMM personality

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

Figure 4-2 – FSC-SMM Personality Download



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

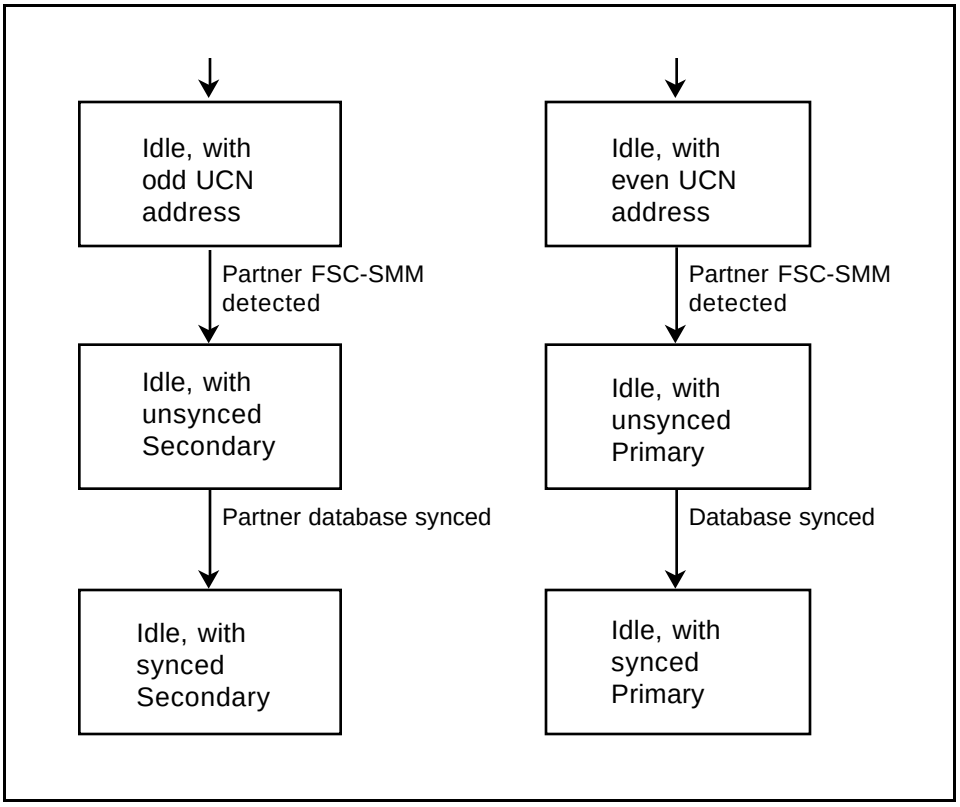
Continued on next page

Cold start-up - FSC-SMM idle state

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

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

Figure 4-3 – Primary/Secondary Idle State Synchronization



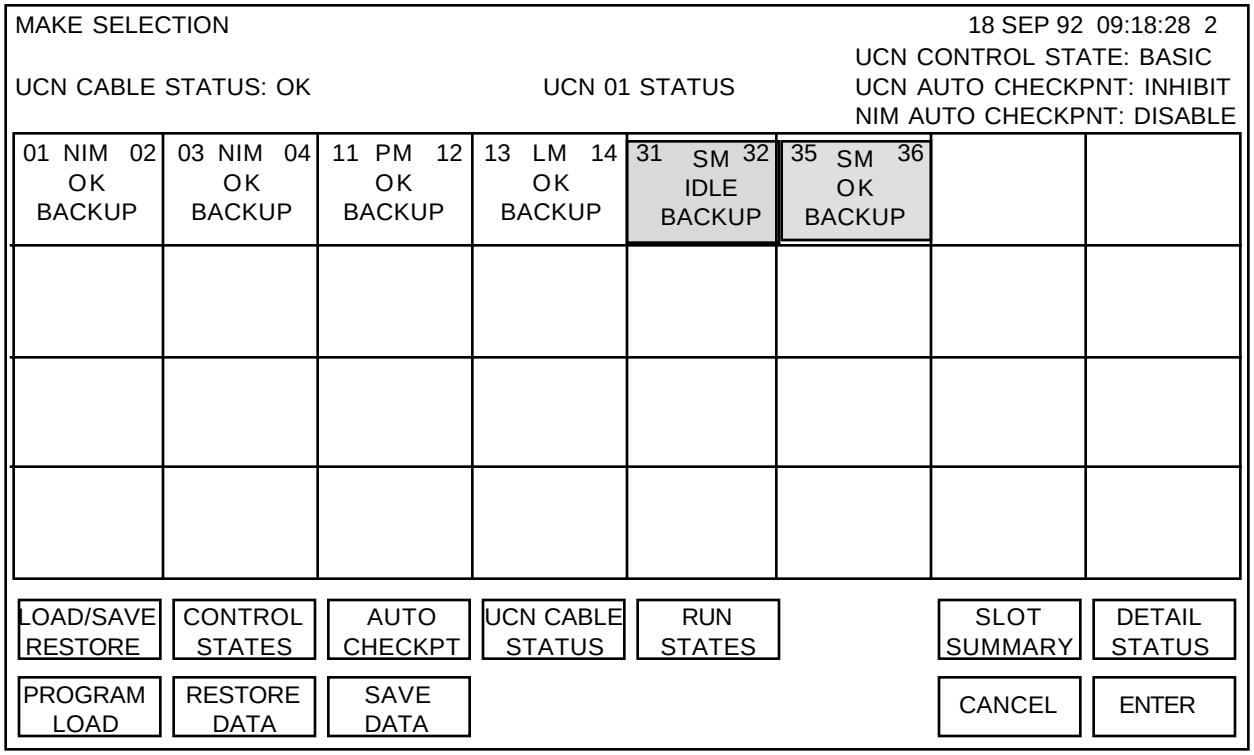
Continued on next page

Cold start-up - FSC-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 FSC-SMMs have reached synchronization state. Note the “IDLE” or “OK” for the Primary and “BACKUP” for the Secondary.

Figure 4-4 – FSC-SMM UCN Status Display Synchronized State



4.2 Warm Start-up

Warm start-up

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

FSC-SMM IDLE/RUN state - warm start-up

With warm start-up following power-up reset, the FSC-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 FSC-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).

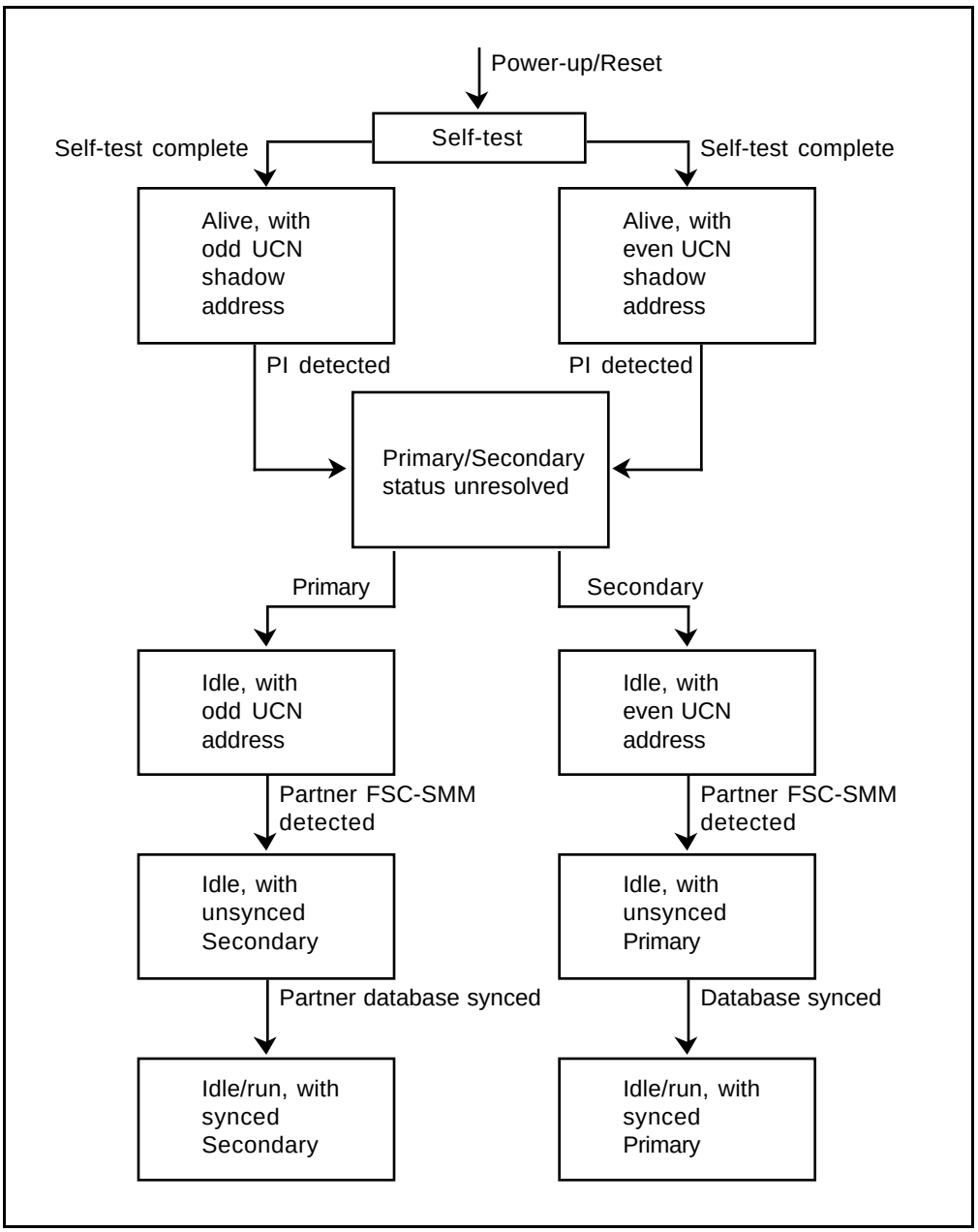
ATTENTION The new Secondary, when swapped, will not perform any self-test (fast restart).

Continued on next page

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

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

Figure 4-5 – FSC SMM Idle State - Warm Start-up



4.3 Shutdown

Shutdown

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

Table 4-1 – FSC-SMM Shutdown

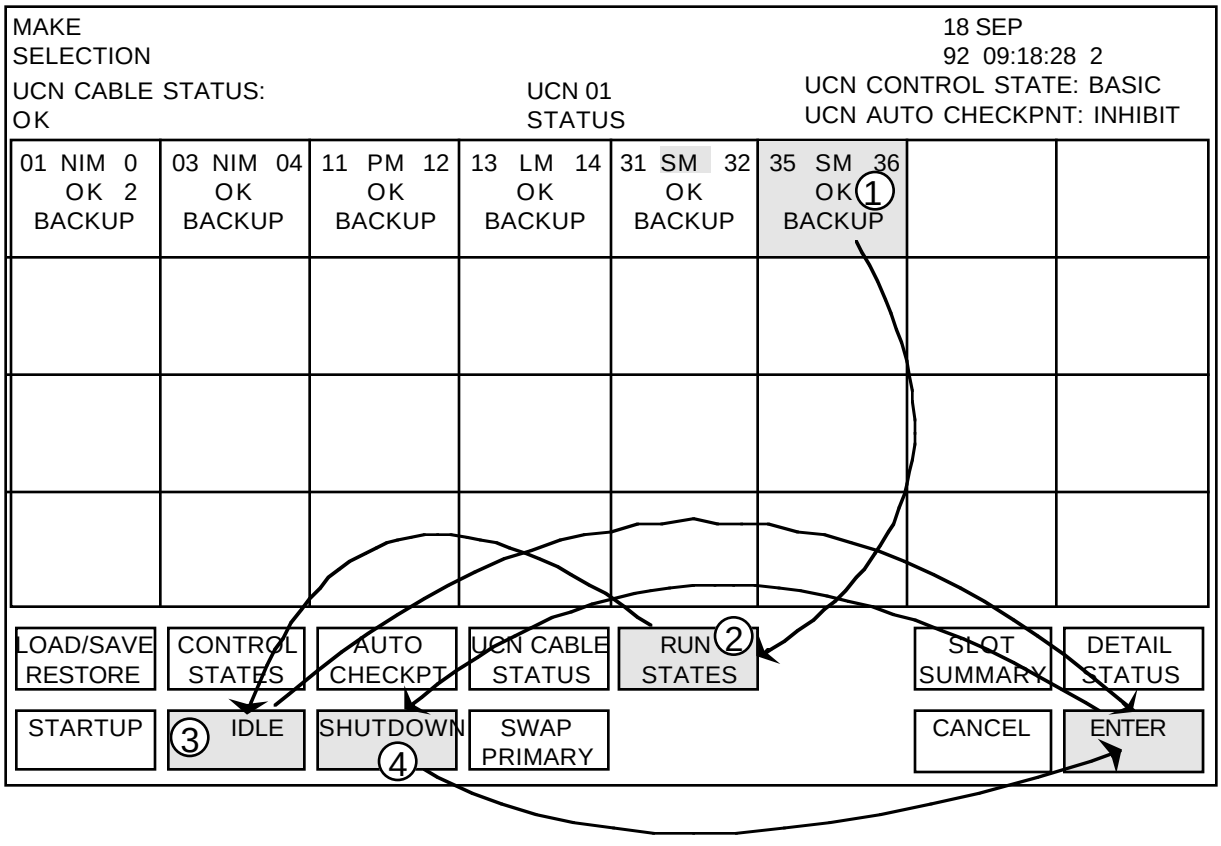
Step	Action
1	Select the targeted node from the screen shown in Figure 4-6.
2	Select the “RUN STATES” target.
3	Select “IDLE” target, then select “ENTER.”
4	Select the “SHUTDOWN” target, then select “ENTER.”

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 FSC-SMM shutdown.

Figure 4-6 – FSC-SMM Shutdown UCN Status Display



Left blank intentionally

Section 5 – Performance Specifications

5.1 FSC-SMM Processor Resource Allocation

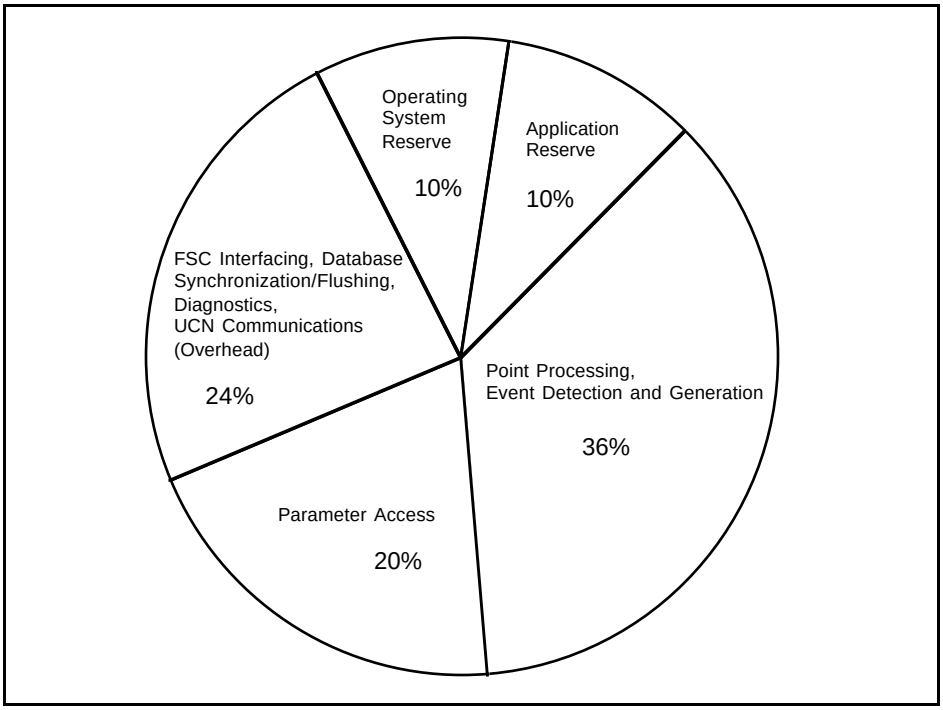
Section summary

This section contains the following topics:

Performance specifications summary

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

Figure 5-1 – FSC-SMM Processor Resource Allocation



Overhead

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

- FSC Control Processor interfacing,
- diagnostics and status, and
- redundancy and checkpointing.

5.2 Performance Statistics

Performance specifications

Table 5-1 outlines the performance specifications for the FSC 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 210 Kbyte
Self-diagnostics	Every 60 seconds
Failover	5 seconds
Primary/Secondary Switchover and Point Process Priming	2 seconds
SOE Resolution	FSC Control Program scan time

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

5.3 Processing Units

Processing units for the FSC-SMM

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

Table 5-2 - Processing Units for the FSC-SMM

Point Type	Processing Units per Point for 0.5 s scan period	Processing Units per Point for 1 s scan period
Digital Input	3.3	1.65
Digital Output	1.8	0.9
Digital Composite	13.5	6.75
Analog Input	17.6	8.8
Analog Output	4.4	2.2
Logic Slot	300	150
Flag (SLOTNUM ≤ 512)	0	0
Flag (SLOTNUM > 512)	0	0
Numeric	0	0
Timer	2.6	1.3

Left blank intentionally

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 an NIM processing load estimate. In this example, the total induced load is 335, which is 33.5% of the maximum load allowed for an 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		1	10	10
PMs, LMs and SMs on UCN	Number of PMs, LMs and SMs on UCN			
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 which 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 spreadsheet 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

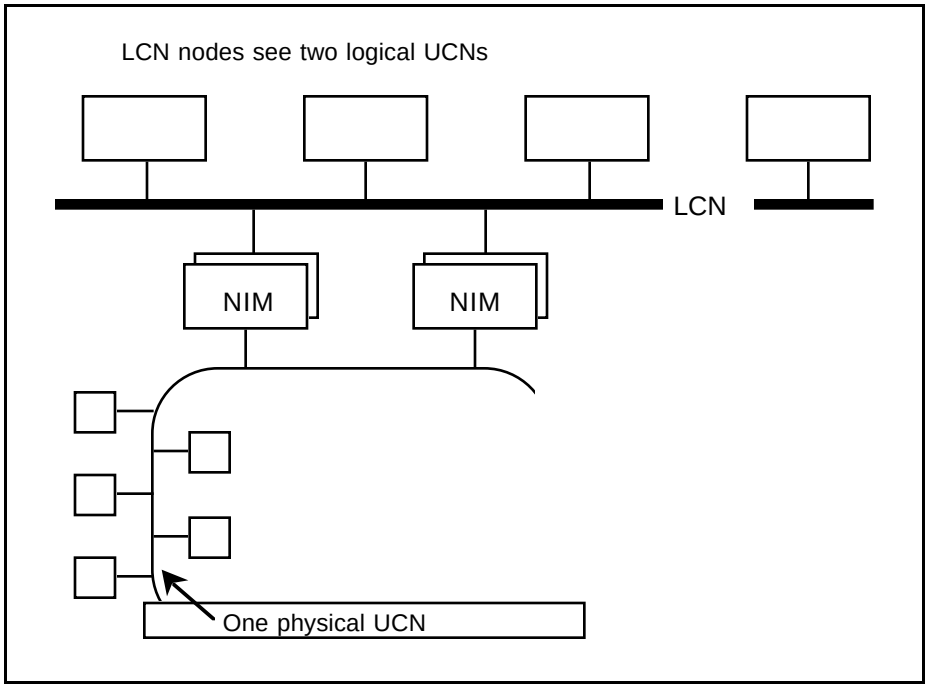
Induced Load	Performance Rating	Result
750 (75%)	Performance as Specified	Will perform as specified under all actual system use conditions.
750 to 1000 (75% to 100%)	Marginally Acceptable	Display of information from this NIM and its reporting of events may occasionally be sluggish, especially during 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 the range from 1 to 20; each UCN and each Data Highway is one process network).
- NIM 2 (configured as RemotNIM) - assigned to process network 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.

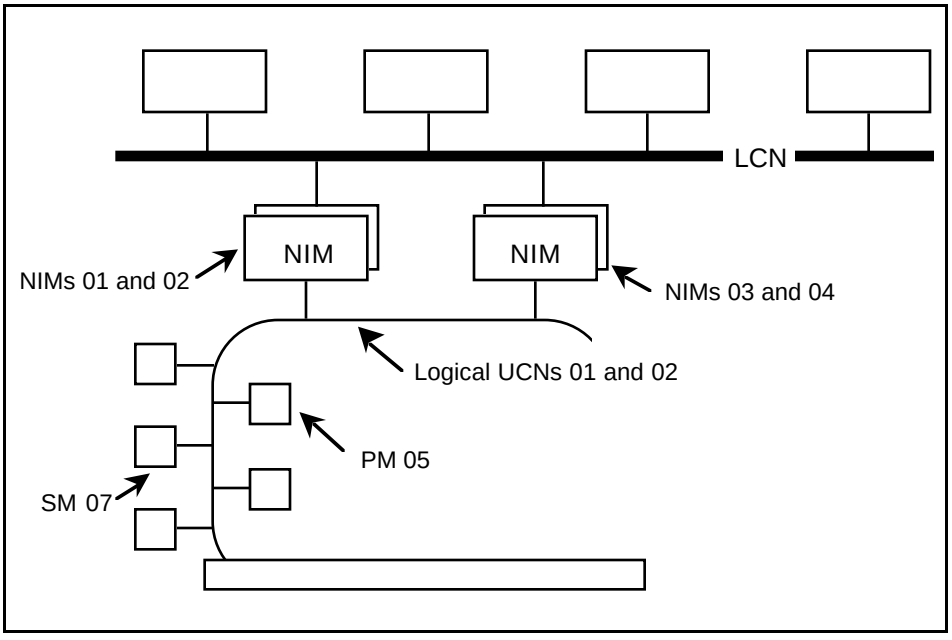
Table 6-4 – Implementation of Two Logical Process Networks

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
SM07	01	$NM01N07	RemotNIM	$NM01B07
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
SM07	02	$NM02N07	ThisNIM	$NM02B07

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 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 FSC-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.

Left blank intentionally

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 FSC-SM (non-redundant and redundant).

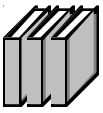
The UCN and LCN points are reserved entities (see Subsection 2.1 of the Data Entity Builder Manual). These entities must be built and loaded before data points can be loaded into the UCN nodes.

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.



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

Continued on next page

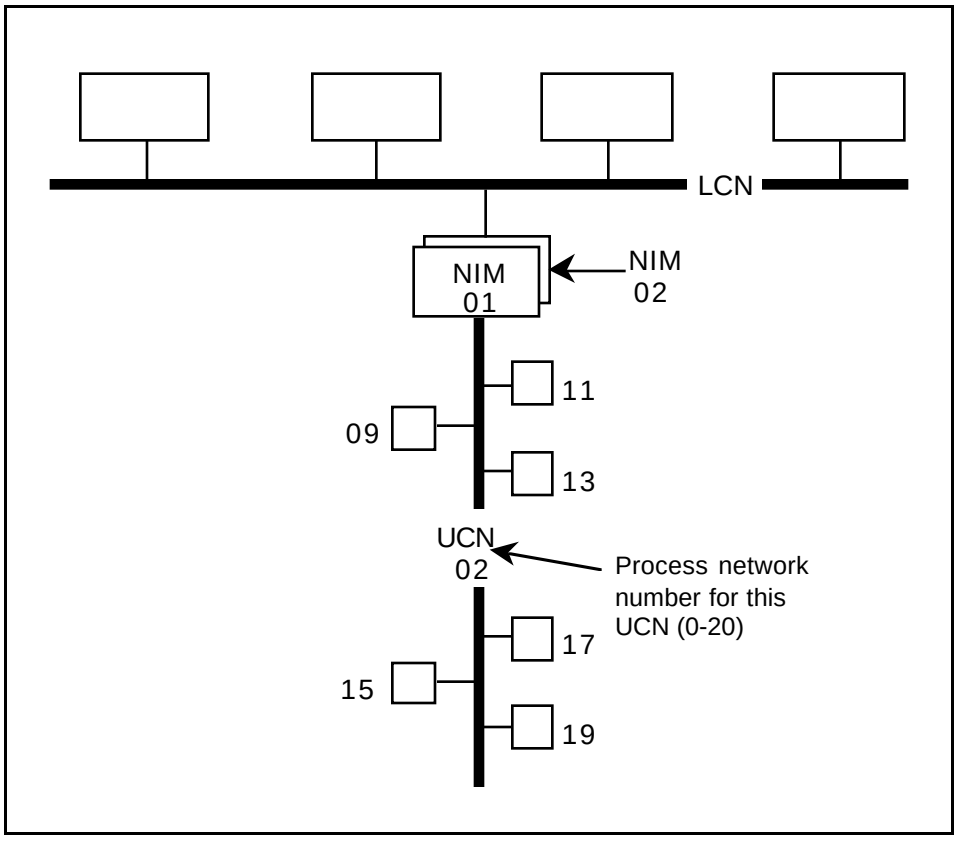
UCN point building example

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
FSC-SM (or PM, LM), node no. 9	$NM02N09	$NM02B09

Figure 7-1 – UCN Node Configuration

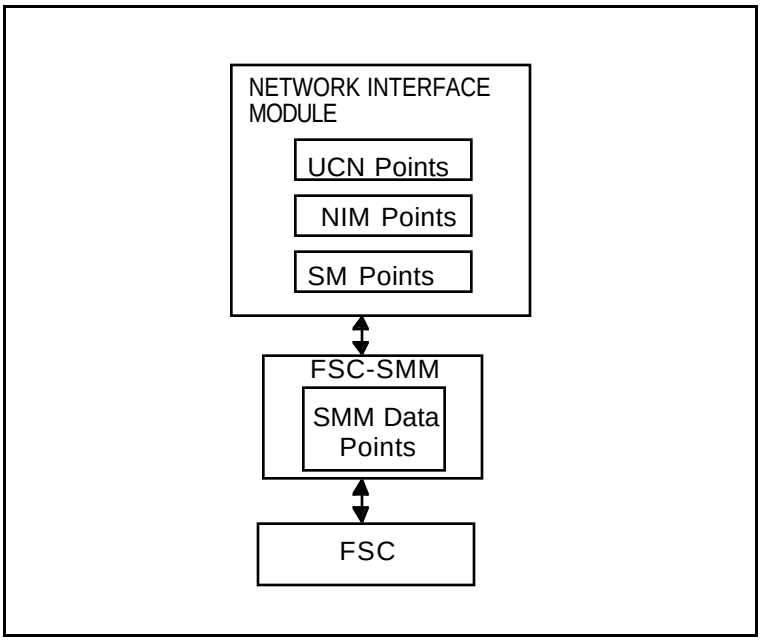


7.2 Node-specific Point Building

Node-specific point building summary

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

Figure 7-2 – FSC-SM Implementation Dependencies



FSC-SMM database

The FSC Safety Manager Module database is configured from the Universal Station. Once loaded into the FSC Safety Manager, this FSC-SMM configuration data can be saved on the History Module and downloaded over the UCN to the FSC-SMM.

Functional Logic Diagram database

The FLD Control Program for the FSC is developed using the FSC Development System. Once loaded in the memory of the FSC Control Processors, the control programs are saved in the FSC-DS database, which can save multiple FLD programs under separate file names.

ATTENTION All diagnostic information that is provided in the FSC is available at the US.

Continued on next page

Determining total FSC-SMM processing units

The maximum number of Processing Units for the FSC-SMM is 6000. 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	3.3	X	_____	=	_____
1.0 sec. digital scan		1.65	X	_____	=	_____
Digital Output 0.5 sec. digital scan	2000	1.8	X	_____	=	_____
1.0 sec. digital scan		0.9	X	_____	=	_____
Digital Composite 0.5 sec. digital scan	1000	13.5	X	_____	=	_____
1.0 sec. digital scan		6.75	X	_____	=	_____
Analog Input 0.5 sec. analog scan	1000	17.6	X	_____	=	_____
1.0 sec. analog scan		8.8	X	_____	=	_____
Analog Output 0.5-sec. analog scan	1000	4.4	X	_____	=	_____
1.0 sec. analog scan		2.2	X	_____	=	_____
Logic 0.5 sec. digital scan	30	300	X	_____	=	_____
1.0 sec. digital scan		150	X	_____	=	_____
Timer 0.5 sec. digital scan	1500	2.6	X	_____	=	_____
1.0 sec. digital scan		1.3	X	_____	=	_____
				POINT PROCESSING TOTAL		_____

Continued on next page

Determining total FSC-SMM processing units, continued

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

- 0.5 sec. digital scan when scan rate = AR1DT2 or AR2DT2.
  1.0 sec. digital scan when scan rate = AR1DT1.
  0.5 sec. analog scan when scan rate = AR2DT2.
  1.0 sec. analog scan when scan rate = AR1DT2.
- The Point Processing total must be 6000 or less to be valid.
- The maximum number of connections between FSC-SMM points and FSC variables is 2000, excluding connections made via flag and numeric points.
- 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 Table 7-2 may be reproduced for use as a configuration worksheet.

Node-specific building displays

Figure 7-3 and Figure 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)

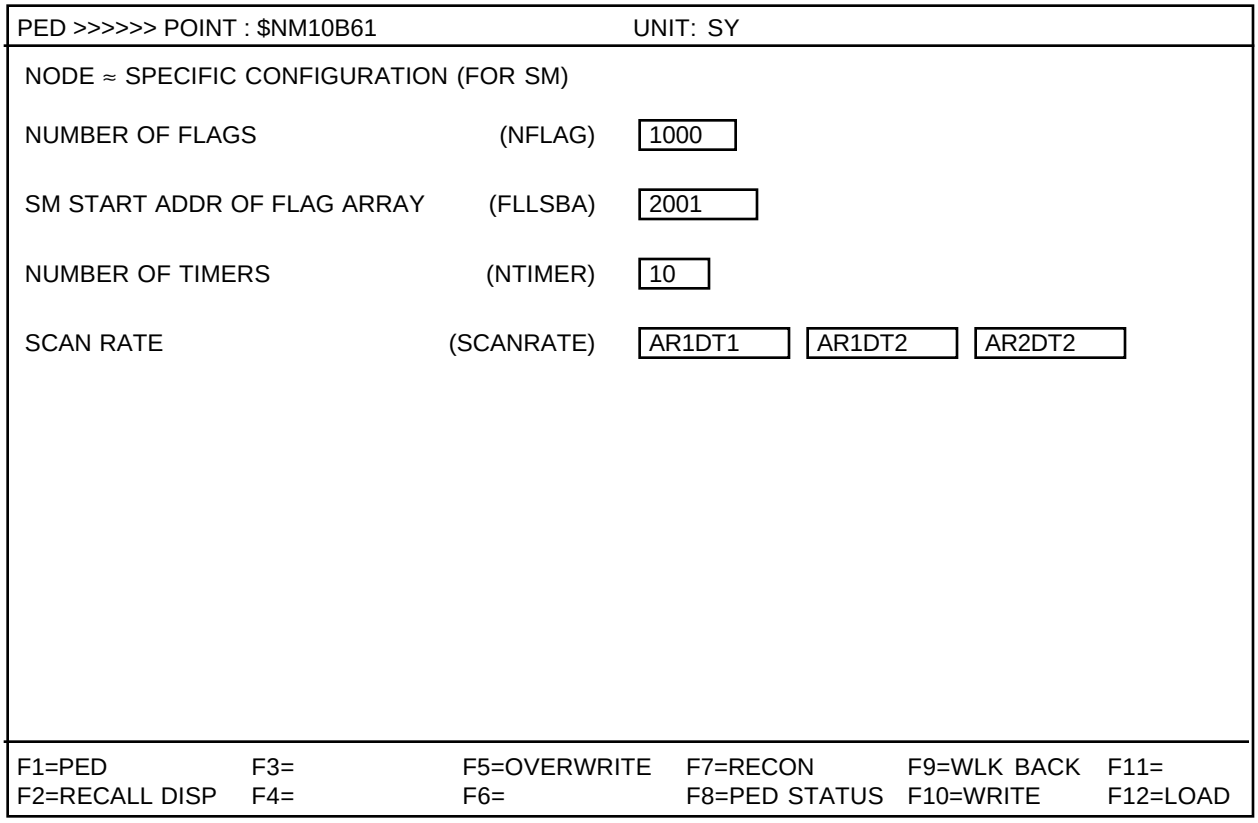
NUMBER OF ANALOG INPUT SLOTS	(NAISLOT)	100
NUMBER OF ANALOG OUTPUT SLOTS	(NAOSLOT)	5
NUMBER OF DIGITAL INPUT SLOTS	(NDISLOT)	600
NUMBER OF DIGITAL OUTPUT SLOTS	(NDOSLOT)	400
NUMBER OF LOGIC SLOTS	(NLOGSLOT)	20
NUMBER OF DIG. COMPOSITE SLOTS	(NDCSLOT)	80
DIG. COMPOSITE NONE STATE	(NONETXT)	NONE
NUMBER 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

Continued on next page

Node-specific building displays, continued

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



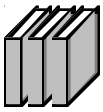
7.3 Box Configuration

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. Refer to the *FSC Safety Manager Control Functions* manual for information about each point type. **ATTENTION** FSC-SMM output points cannot be mapped to FSC outputs. FSC programming (i.e. FLD) will be required to affect real output control and can only be done through the FSC-DS.
5	Select the Parameter Entry screen displays. Enter parameters. Refer to FSC Safety Manager Parameter Reference Dictionary for parameter details.



Refer to the *FSC Safety Manager Installation Guide* in this binder for US configuration of FSC-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.

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.

An FSC Safety Manager softfail may have many different causes.

Continued on next page

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 FSC-SMM Diagnostic Displays	FSC-SMM Interpretation and/or Comments
19	UCNPRSFL	Pri Cannot Talk to Sec on UCN	FSC-SMM has lost the ability to communicate over the UCN.
20	UCNSCPFL	Sec Cannot Talk to Pri on UCN	FSC-SMM has lost the ability to communicate over the UCN.
21	NOSYNCH	Secondary Not Synced	Loss of FSC-SMM Redundancy.
34	UCNOVRUN	UCN Overrun	FSC-SMM unable to prefetch data from remote nodes (peer-to-peer inputs).
35	PPXOVRUN	Point Processor Overrun	FSC-SMM point scanning is lagging behind schedule.
54	LCLLNOSC	LC Not Scanning	FSC-SMM Point Processing requires the Logic Controller to scan its inputs and its user program.
63	LCIOCDFL	LC Comm or I/O Card Fault	FSC System Aliases are signaling an I/O fault.
80	SMTSFLT	FSC-SMM Time Synch Failure	Set by an FSC-SMM upon detection of a UCN Time Sync failure. Causes include: • UCN Time Sync hardware/software failure.
81	LCTSFLT	LC Time Synch Failure	Set by an FSC-SMM upon detection of a Logic Controller Time Sync error. Causes include: • FSC Time Sync hardware failure. • FSC Time Sync command processing failure.

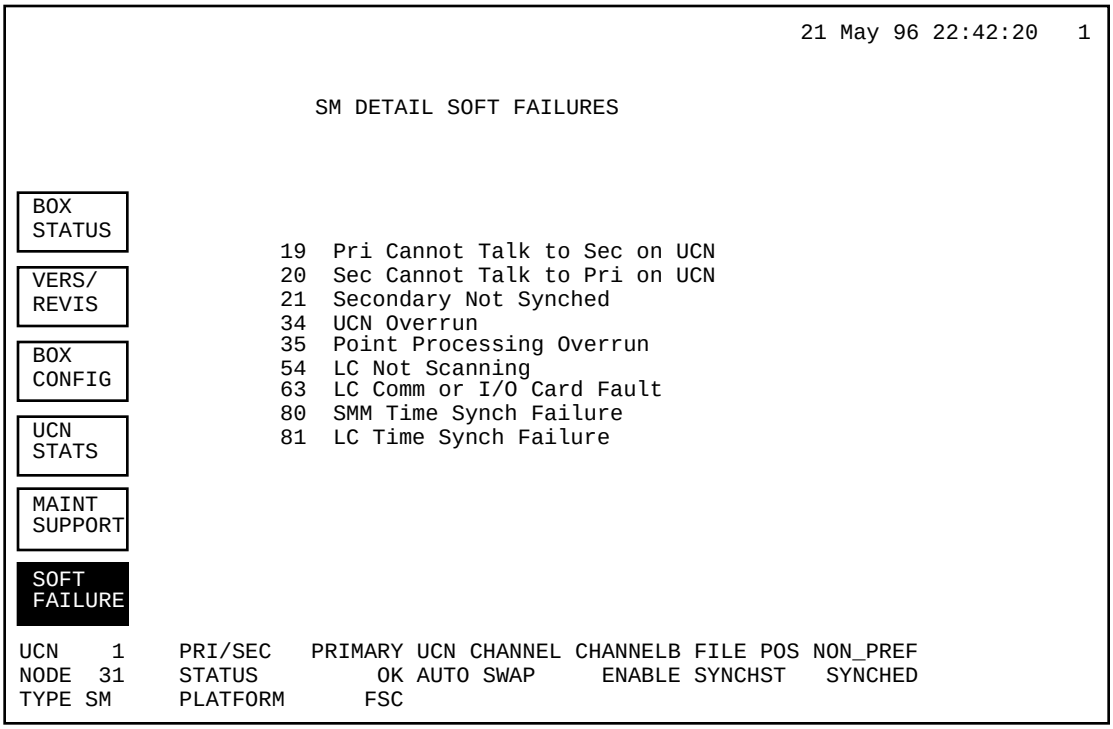
Continued on next page

Soft failures US display

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

ATTENTION Active soft failures will be highlighted.

Figure 8-1 – US Display: Soft Failures



8.2 Hard Failures

Hard failures summary

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

- component failure,
- program or database failure.

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

Table 8-2 – Configuration Errors

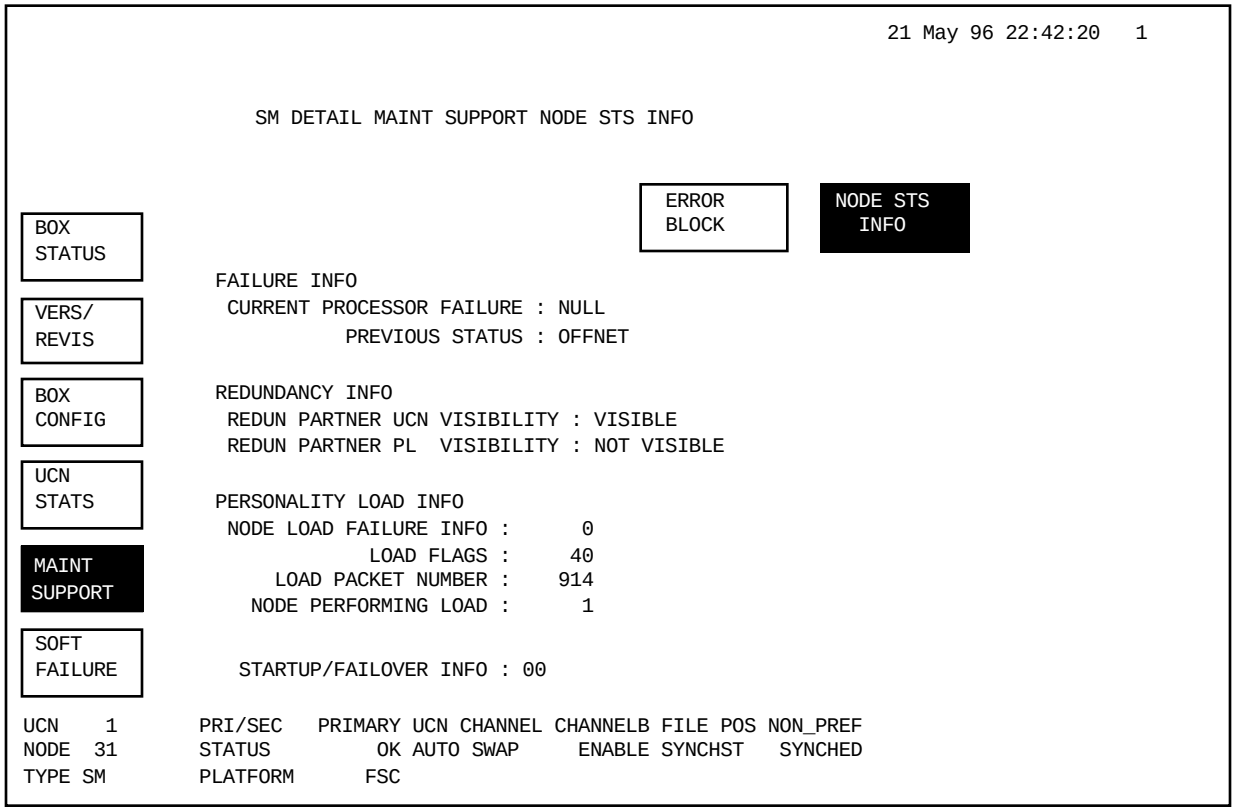
Error	Description
ILLEGAL VALUE	Attempted to write an FSC hardware addressing parameter (e.g. PLCADDR, LODSTN, CCSRC, ILCxxxxx, etc.) which specifies an Alias not available within the host FSC.
READ ONLY	Response to attempts to write to a read-only FSC-SM parameter.
CONFIGURATION MISMATCH	An invalid 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 "NODE STS INFO" target.

Figure 8-2 – US Display: NODE STS INFO Target

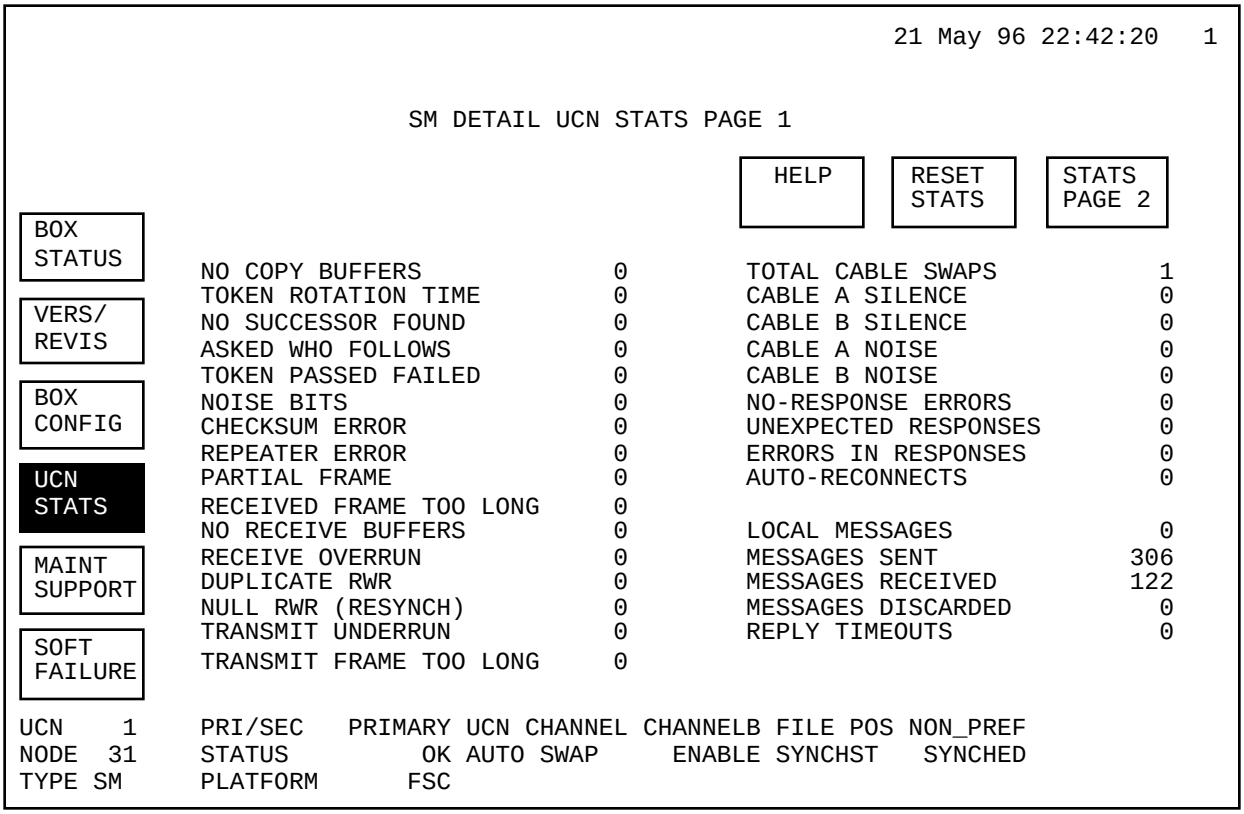


Continued on next page

US display showing UCN statistics

Figure 8-3 shows the US UCN statistics 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: UCN Statistics Screen, Page 1



UCN addressing errors

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

Left blank intentionally

Index

Index

J, K

L, M

N

O

P, Q

R

S

T

U

V

W, X, Y, Z

READER COMMENTS

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

You can communicate your thoughts to us by fax or mail using this form, or by placing a toll-free telephone call. We would like to acknowledge your comments—please include your complete name, address, and telephone number.

BY FAX: Use this form and fax to us at 1-602-313-4108.

BY TELEPHONE: In the USA, 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 and mail to us at:

Honeywell Inc.
Industrial Automation and Control
Automation College
2820 West Kelton Lane
Phoenix, AZ 85023-3028

Title of Document:	**FSC Safety Manager Implementation Guidelines**	Issue Date:	**09/96**
Document Number:	**FS11-500**	Writer:	**HSMS Product Marketing**

COMMENTS: _____

_____

_____

_____

_____

_____

_____

RECOMMENDATIONS: _____

_____

_____

_____

_____

_____

_____

Name: _____ **Date:** _____

Title: _____

Company: _____

Address: _____

City: _____ **State:** _____ **ZIP:** _____

Telephone: _____ **FAX:** _____

Honeywell

Industrial Automation and Control
Honeywell Inc.
16404 North Black Canyon Highway
Phoenix, Arizona 85023-3033

Helping You Control Your World