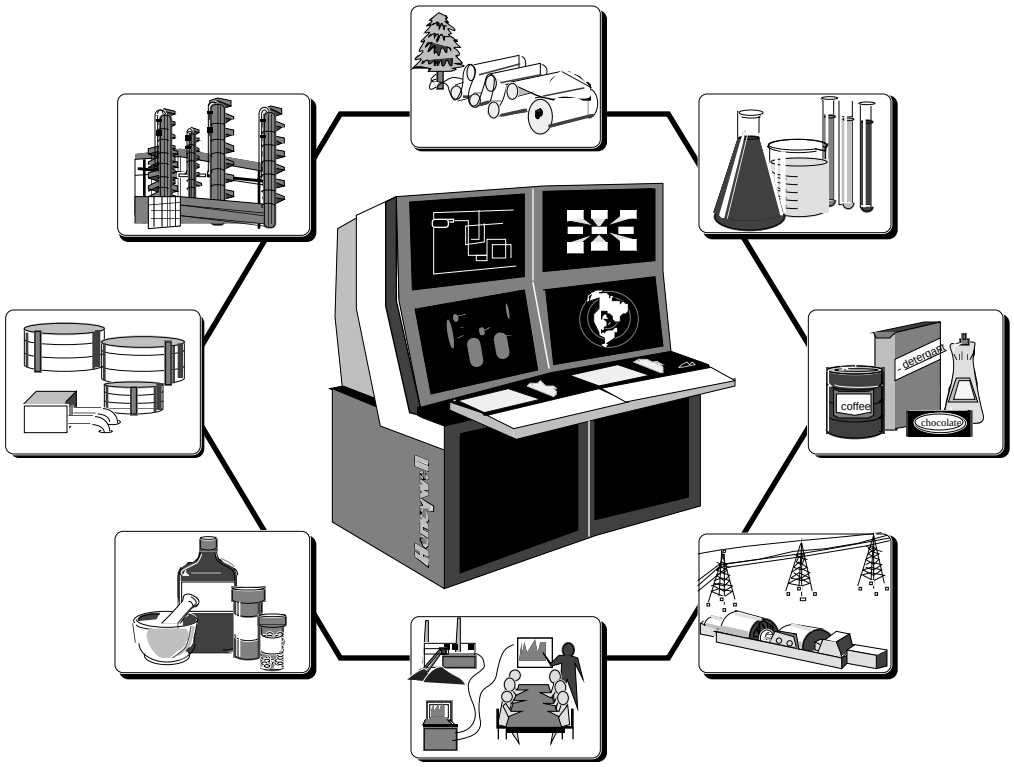
Honeywell

FSC Safety Manager Specification and Technical Data

FS03-500
1/97



Total Plant

FSC Safety Manager for FSC Release 400

Specification and Technical Data

TABLE OF CONTENTS **Page**

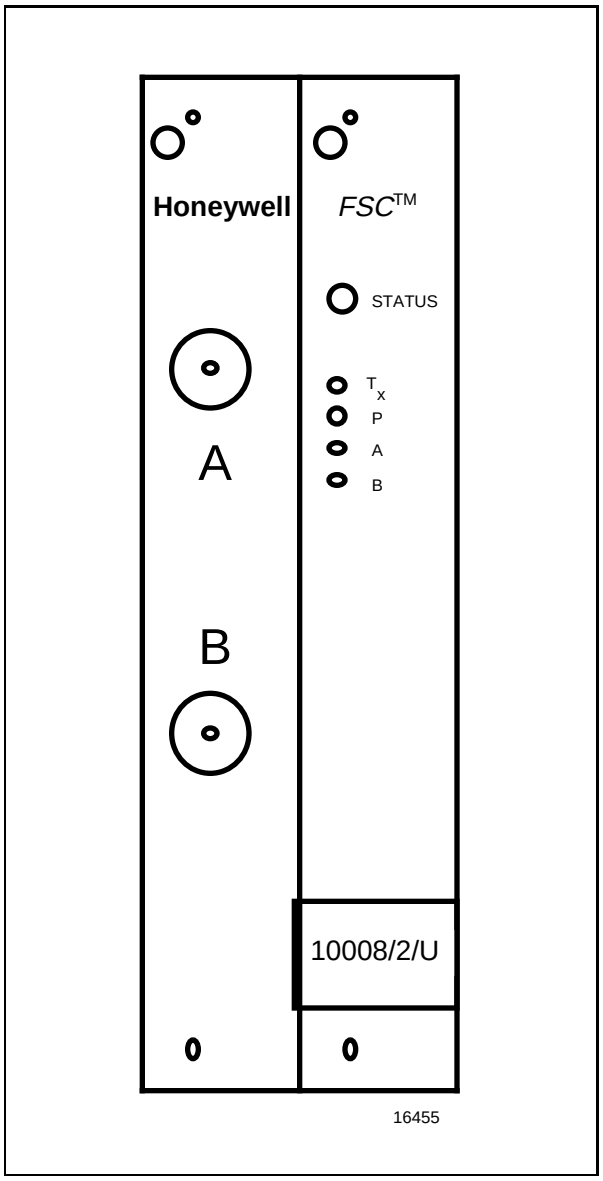


Figure 1 — FSC Safety Manager Module

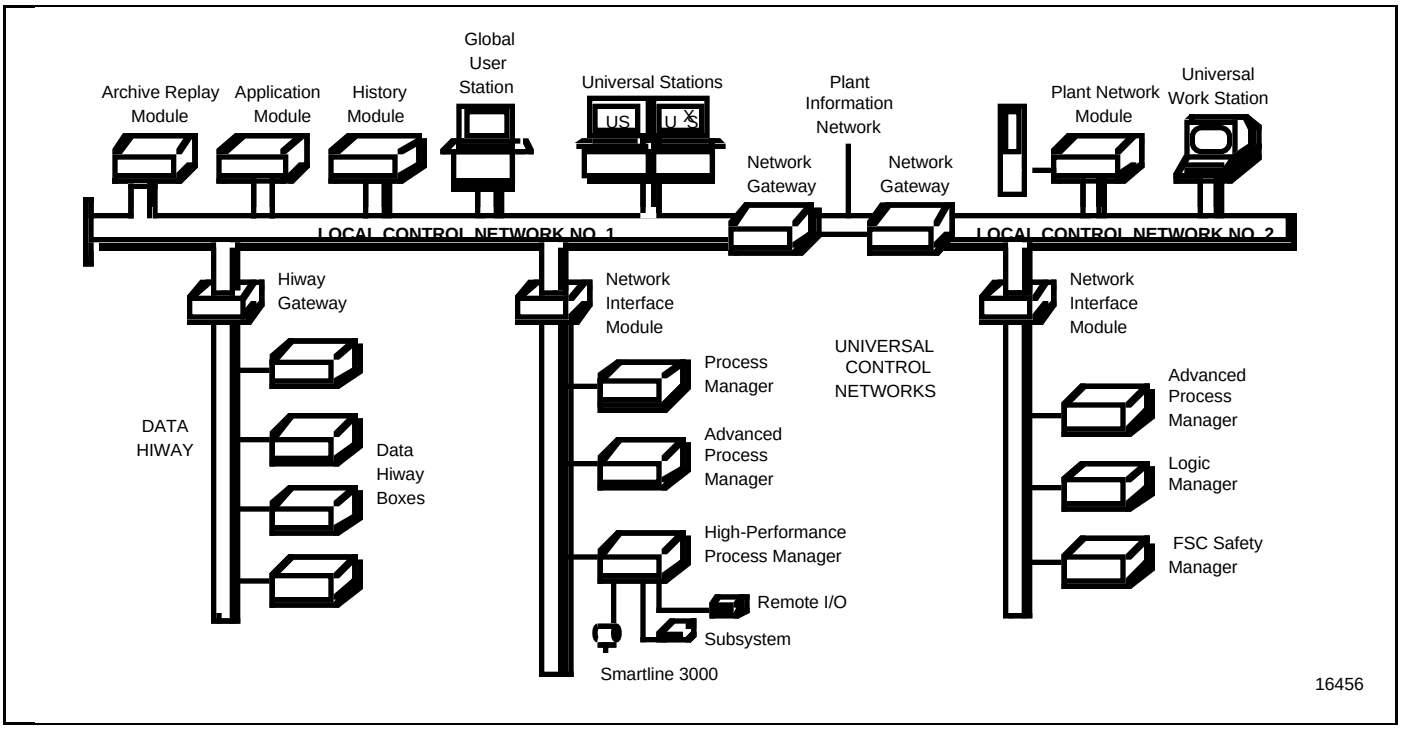


Figure 2 — TPS Architecture

INTRODUCTION

The FSC Safety Manager (FSC-SM) provides a dual redundant fault-tolerant controller for safety and shutdown applications on the **TotalPlant** Solution (TPS) system's Universal Control Network (UCN). It consists of a Honeywell FSC™ controller equipped with an FSC Safety Manager Module (FSC-SMM) interface card. The specification and the technical data contained in this document mostly concerns the FSC-SMM. For detailed specifications and technical data on an FSC system, please refer to the FSC documentation.

In line with Honeywell's philosophy of consistent product evolution, the FSC Safety Manager adds yet another powerful element to the TPS advanced system for industrial control. Safety functions are now integrated into the architecture of the Universal Control Network (UCN) to support integrated operations and control. The result is a true TPS-based window into the FSC; the powerful safety system which has superior uptime and safety-related performance for applications such as:

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

Because of its integration into the Universal Control Network, as shown in Figure 2, the FSC Safety Manager shares important features with its UCN peers. They include:

- direct peer-to-peer communication with other Safety Managers, Process Managers, Advanced Process Managers, High-Performance Process Managers, and Logic Managers (initiated by either an SM, PM, APM, HPM, or LM),
- communication with operators, engineers and maintenance personnel at the TPS operator stations (i.e., Universal Stations, U^{X}Ss, Universal Work Stations, and Global User Stations),
- support of higher-level strategies through communication with Application Modules and host computers on the Local Control Network, and
- FSC-SMM database restoration from the History Module.

Universal Control Network

The communications channel for the FSC Safety Manager to the TPS system is a local area network called the Universal Control Network (UCN). Introduced to TDC 3000^X users in 1988, the UCN is the secure path for process I/O connections to the TDC 3000^X and its successor, the **TotalPlant** Solution (TPS) system.

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

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

Network Interface Module

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

LCN time and UCN time are synchronized by the NIM. The NIM broadcasts LCN time over the UCN. The FSC-SM (as well as HPM and APM) uses it for all alarm (event) timestamping and for DI SOE time synchronization.

FUNCTIONAL DESCRIPTION

Functional Overview

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

The FSC control processors read the process inputs and execute the control program written by the user in graphical Functional Logic Diagrams (FLDs). Inputs are polled and synchronized by the FSC control processors, processed by the control program and then transmitted to the output modules.

Continuous self-tests of the FSC hardware by the FSC control processor ensure safe control of the process and adequate system and process equipment diagnostics.

The FSC-SM has a typical application cycle of 300 milliseconds. Every scan cycle of the FSC control processor's control program cycle, the FSC control processor scans and updates the FSC-SMM to exchange information between the Control Program and UCN. The FSC-SMM converts this

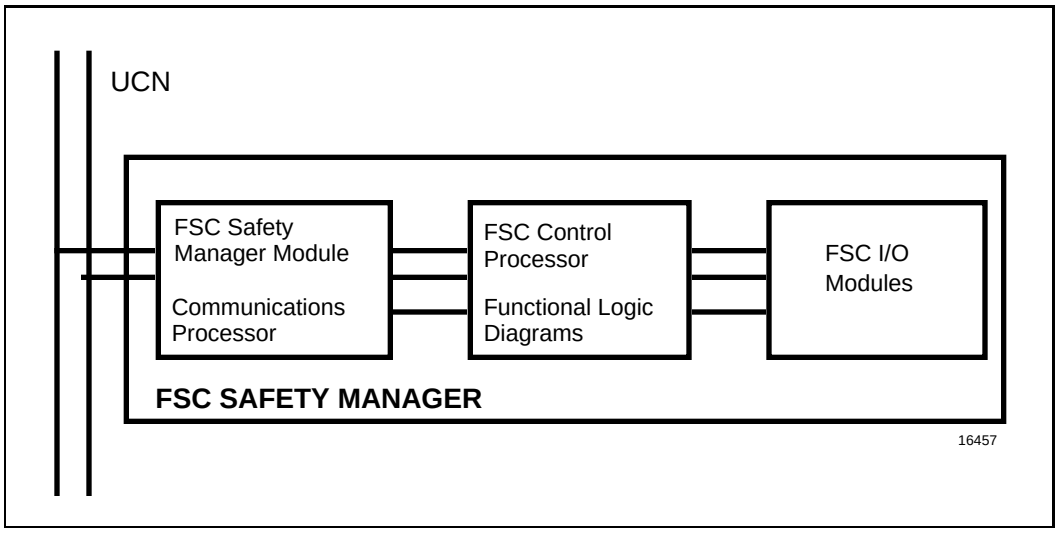


Figure 3 — FSC Safety Manager Architecture

* Institute of Electrical and Electronics Engineers

** International Standards Organization

Point Type	Maximum number	PUs/Pt. @ 0.5 sec.	Safety Manager PU Loading				
			Point Type	Scan Time 1 sec.	PUs/PT	PT. Qty	Total PUs
Analog Input	1000	17.6	Analog Input	1.0	8.8	70	616
Analog Output	1000	4.4	Analog Output	1.0	2.2	35	77
Digital Input	2000	3.3	Digital Input	1.0	1.65	700	1155
Digital Output	2000	1.8	Digital Output	1.0	0.9	350	315
Digital Composite	1000	13.5	Digital Composite	1.0	6.75	200	1350
Timer	1500	2.6	Timer	1.0	1.3	30	39
Logic Point	30	300	Logic Point	1.0	150	5	750
Flags	2000	0	FSC-SMM Total			1390	4302
Numerics	1000	0	Maximum Number				6000
			Flags & Numerics are not listed, since their PU weights are 0.				

Table 1 – Maximum Number of Each Data Point Type Per FSC-SMM with PU Load and Example

data to UCN data types (Tag.Parameter), performing engineering unit conversion, alarm handling, annunciation, diagnostic status reporting and UCN communication functions. The FSC-SMM scan cycle can be 0.5 or 1 second.

Operator changes from the TPS operator stations are written to the FSC control program via dedicated boolean and numerical inputs. The inputs appear at the input side of the Functional Logic Diagrams, where the conditions for write access are defined. This results in a true integration of safety-critical control functions within the TPS context.

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.

The control program for FSC Control Processors is developed using the FSC Development System (FSC-DS). Once loaded into the memory of the FSC control processors, the control programs are saved in the FSC-DS database. In addition to integration of Safety Manager data points into standard TPS operator station displays, additional displays are available for maintenance. All diagnostic information that is provided in the FSC controller is available at the TPS operator stations.

Data Point Types

Table 1 shows the FSC-SMM point types and their related maximum number of points per FSC-SMM. Please note that the total maximum number of all points added together cannot be used with one FSC-SMM. A mixture of point types and their related load on the system must be considered by adding the total Processing Units (PUs)/Point so as not to exceed 6000 for the normal scan rate of 0.5 seconds.

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

Digital Input*:* An FSC Safety Manager Module digital input (DI) can be acquired from any designated DI status location within the FSC controller. Typically, it would be mapped to a Hardware Input Channel which contains the status of a process connection.

Digital Output*:* Upon receipt of a digital output (DO) request from a system device, the FSC-SMM records the demanded status in its "current status table." The FSC control processor scans the table contents and includes the status in

the control program. This is true only if the DO point is connected to an FSC boolean input variable dedicated to receive data from communication devices.

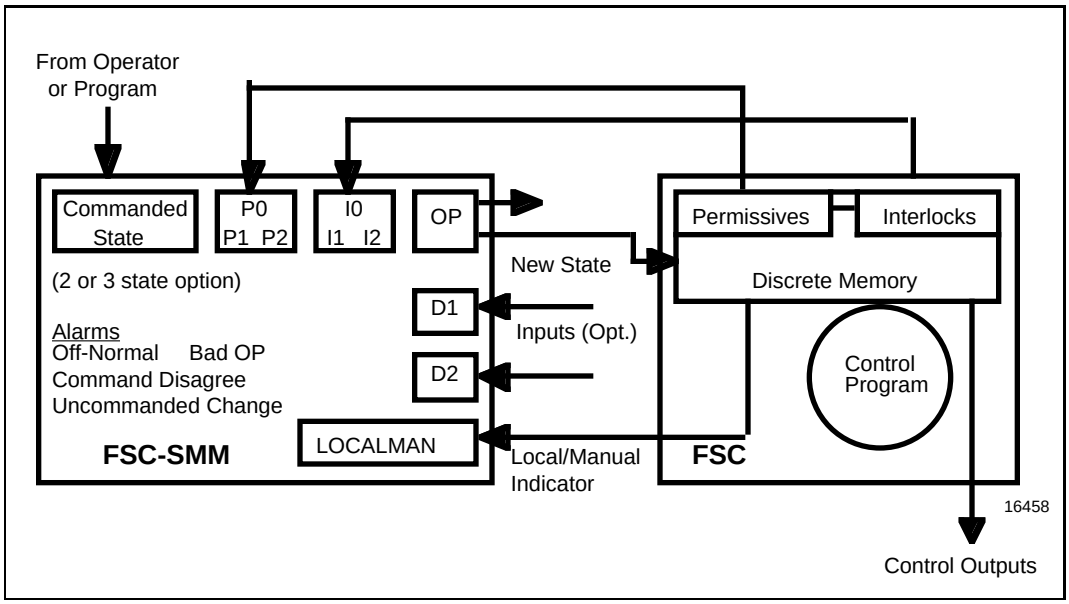


Figure 4 — Example Showing Digital Composite Point Data Flow

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

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

***Analog Outputs**:* An analog output (AO) from the UCN is converted by the FSC-SMM to the FSC format, and then queued as a "write command" for the designated FSC numerical input variable. This will be processed during the next control program scan. Again, this is only true if the AO point is connected to an FSC numerical input variable dedicated to receive data from a communication device.

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

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

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

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

Alarm System Functions

The FSC Safety Manager Module supports the extensive alarming features of the TPS system. As process alarms are detected, they are brought to the operator's attention at the Universal Station through keyboard LEDs and a variety of displays including alarm summaries, alarm annunciator displays, group displays, and custom graphic displays. Because

alarms can be configured to selected areas or units, operators need not be subjected to alarms that do not relate to their specific assignments.

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

Point Processing

All data being transferred between the FSC-SMM and the FSC controller can be configured to be updated with either a 0.5 or 1 second scan cycle. At a 0.5 second scan rate, the PU loading is set to a maximum of 6000. Point counts can be doubled by increasing the scan rate. Actual control program processing typically occurs at much faster rates. Operator output changes are processed immediately by the FSC-SMM.

The FSC control processor includes the value in the control program if connected to an input dedicated for reception of data from communication devices.

Peer-to-Peer Communications

The FSC Safety Manager Module provides the ability to implement inter-node process control strategies between the SM and other UCN nodes such as LM, PM, APM, HPM or another SM. These transactions are initiated via the logic point. There are 12 enabled links per point and with up to 30 points permitted. There is a limit of 50 UCN input (fetch) connections and 50 UCN stores per FSC-SMM scan at the 0.5 second standard scan rate. The FSC-SMM scan rate can be set to 1 second, which increases the UCN input connections and UCN stores to 100 per FSC-SMM.

FSC Safety Manager Module Redundancy

As a standard feature, the FSC Safety Manager Module operates in a dual redundant mode.

Each Central Part of the redundant FSC controller contains its own FSC-SMM through which the Control Processor is capable of communicating with the UCN, independent of the status of the other FSC Control Processor.

Each FSC Safety Manager Module uses dual redundant communication paths to the UCN.

Communication across the UCN is realized via one FSC-SMM at a time, called the primary FSC-SMM. The secondary FSC-SMM is synchronized (database copied) in less than 1 second and its switchover time is less than 1 second (writes to the primary are acknowledged after the secondary receives a copy of the request).

Write Protection

To maintain the safe and reliable operation of the FSC controller, the FSC-SM does not allow direct write access to the FSC outputs.

Write requests, received via the UCN, are passed to the FSC control program via dedicated boolean and numerical inputs. The inputs appear at the input side of the Functional Logic Diagrams, where the conditions for write access are defined.

Displays

The TPS operator station displays this new UCN node on the UCN Status Display as “SM” node with platform “FSC.” Diagnostic displays emulate the FSC Development Systems Extended Diagnostic displays. The displays show failure mode information to the board level.

PHYSICAL CHARACTERISTICS

Standard Configuration

The standard configuration for a redundant FSC Safety Manager consists of:

- Two FSC Central Part racks each with the following modules:
  - Key switch module
  - Power Supply Unit (PSU)
  - Power Supply Distribution module (PSD)
  - Central Processor Unit (CPU)
  - Watchdog module (WD)
  - FSC Safety Manager Module (FSC-SMM)
  - Communication module (COM)
  - Vertical Bus Driver module (VBD)
  - Diagnostic and Battery Module (DBM).

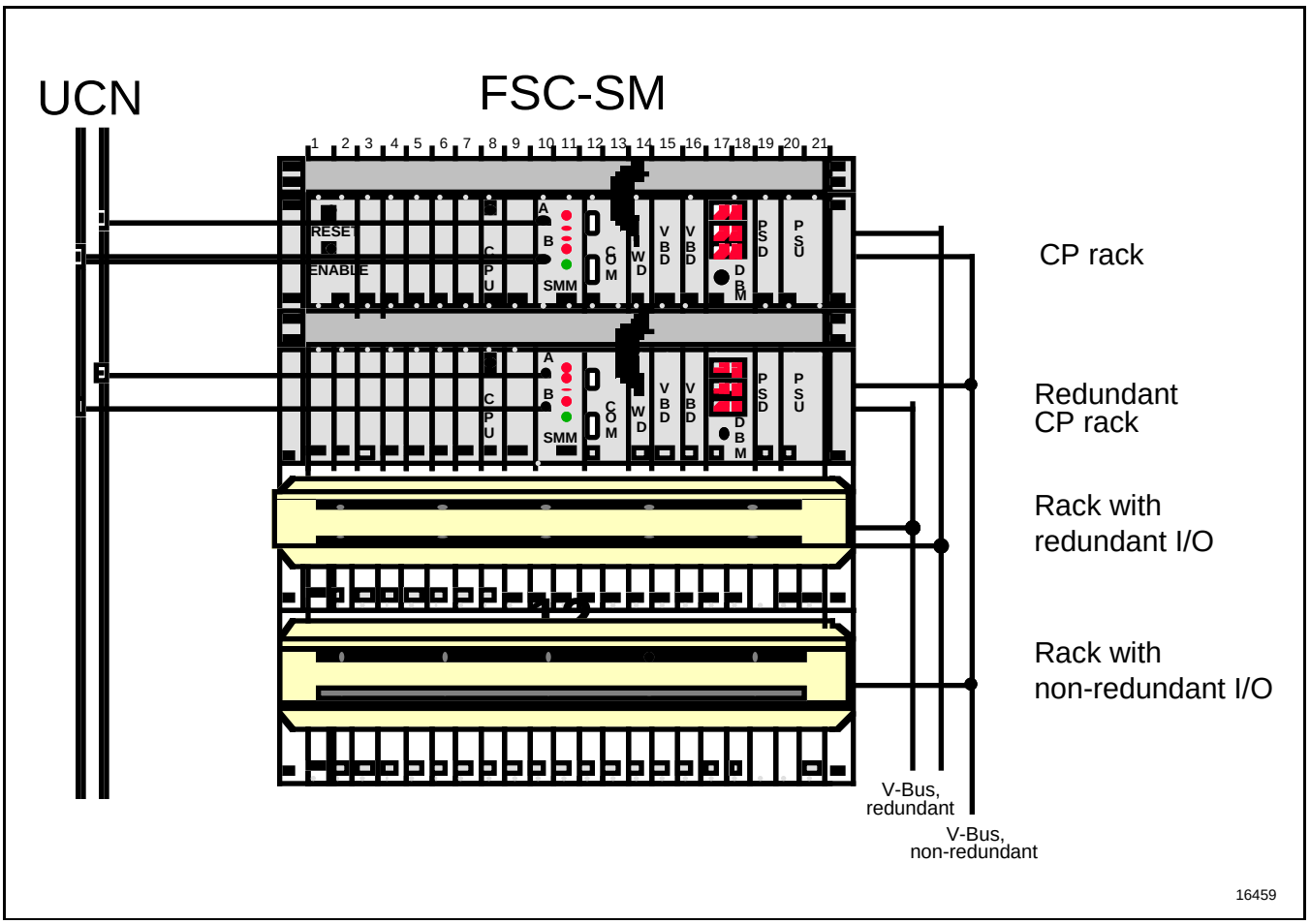


Figure 5 – Typical FSC-SMM layout

- One or more I/O racks containing FSC input and output modules for interfacing with field equipment. Interfaces include:

  Inputs:

  – Digital - 24, 48, and 60 Vdc
  – Digital - 115 Vac
  – Analog
    0(4) - 20 mA
    0(1) - 5 Vdc
    0(2) - 10 Vdc

  Outputs:

  – Digital - 24, 48, 60, 110, and 220 Vdc
  – Digital - 115 Vac
  – Analog
    0(4) - 20 mA
    0(1) - 5 Vdc
    0(2) - 10 Vdc
  – Relay

FSC-SM Layout

Figure 5 illustrates a typical layout of an FSC Safety Manager. The top two racks contain the central parts of the redundant FSC controller.
The FSC Control Processors synchronize their operation via a private Inter Central Part Communication Link. The second channel at the communication module can be used to connect the FSC Development System.
A watchdog module in each central part monitors the operation of its control processor (runtime) and the environment of the control processor (supply voltage, memory integrity), and de-activates the outputs if required.

Each central part is directly connected to the UCN via its own FSC-SMM.

The two bottom racks are I/O racks containing the FSC input and output modules for interfacing with field equipment.

OPTIONS

Sequence of Events (SOE)

The FSC-SMM provides Sequence of Events (SOE) for DI points with the information presented in the standard TPS SOE displays and journals. The resolution of the event data is the scan time of the FSC controller with the time stamp appended by the FSC control processor. FSC Safety Manager time synchronization with the LCN is accomplished as follows: the NIM synchronizes with the LCN, the UCN nodes (e.g., FSC-SMM) synchronize with the NIM, and the FSC control processor synchronizes with the FSC-SMM.

The digital input change-of-state events are time-stamped with the time value received from the FSC control processor. All non-SOE events are time-stamped by the FSC-SMM based on its local clock. The FSC-SMM prioritizes the collection and distribution of non-SOE events over SOE events (such as alarms which need to be distributed over the UCN as quickly as possible) and it must regulate the distribution of events so that no more than 512 SOE events are sent over the UCN in any 10-second period. The FSC-SM provides Event Recovery buffering for the most recent 2000 events.

The FSC-SM SOE does not interfere with the SER (Sequence of Events Recorder) option of the FSC Control Processor, and the SOE configuration is separate from alarm configuration. The FSC-SM can ride through NIM and FSC-SMM failover without loss of SOE events. The FSC-SMM, on transition to RUN state after power-up and subsequent program load or memory retention, must command immediate Event Recovery (similar to the APM). However, it will wait for the first UCN Timesync before issuing the first FSC-SM Timesync, and any SOE events collected during this period must receive a null time stamp.

MISCELLANEOUS

System Requirements

The Honeywell TPS system must be of a Release 510 or higher. The release of the FSC system must be 400 or higher. System upgrade kits are available for both systems.

Model Number

FSC Safety Manager Module model number	10008/2/U

FSC-SM SPECIFICATIONS

Environmental Specifications	
Operating Temperature	0°C to 60°C, ambient*
Storage Temperature	-20°C to 70°C
Relative Humidity	5% to 95%, non-condensing
Vibration, Sinusoidal	IEC 68-2-6; 1 G at 10 to 150 Hz
Shock	IEC 68-2-27; 15 G for 11 ms
Electrostatic Discharge	IEC 801-2, Level 4 (15 KV)
Conducted Susceptibility	IEC 801-4, Level 3, Fast Transient/Burst IEC 801-5, Level 2, Surge Withstand IEC 801-6, Level 3, Conducted Field
Rated Susceptibility	IEC 801-3, Level 3
Conducted Emissions	Measured per CISPR 11 & CISPR 22
Rated Emissions	Measured per CISPR 11 & CISPR 22
* "Ambient" refers to the air temperature measured in the FSC Central Part rack.	

International Standards and Safety Codes

TÜV Bayern:

Certified to fulfill the requirements of "Class 6" safety equipment as defined in the following documents:
Din V VDE 19250, DIN V VDE 0801 A1, DIN VDE 0116/10.89

Canadian Standards Association (CSA) – CSA certied to fulffiill requirements of these two standards:

CSA Standard C22.2 No. 0-M982 General Requirements – Canadian Electrical Code, Part II
CSA Standard C22.2 No. 142-M1987 for Process Control Equipment

Underwriters Laboratories (UL):

Certified to fulfill the requirements of UL-508 and UL-1998 (pending)

CE compliance:

Complies with CE directives 89/336/EEC (EMC) and 73/23/EEC (Low Voltage)

Mechanical Specifications	
Overall dimensions	4 cm x 13 cm x 19 cm (W x H x D) 1.58 in x 5.12 in x 7.48 in (W x H x D)
Approximate weight	400 g (0.9 lb.)

Copyright, Trademarks, and Notices