User Manual
GFK-3277A
Jun 2025

PACSystems™ VersaMax SafetyNet System

SAFETY MANUAL (IC695CPS400 CONTROLLER AND VERSAMAX I/O)

Contents

Warnings and Caution Notes as Used in this Publication

⚠ WARNING

Warning notices are used in this publication to emphasize that hazardous voltages, currents, temperatures, or other conditions that could cause personal injury exist in this equipment or may be associated with its use.

In situations where inattention could cause either personal injury or damage to equipment, a Warning notice is used.

⚠ CAUTION

Caution notices are used where equipment might be damaged if care is not taken.

Note: Notes merely call attention to information that is especially significant to understanding and operating the equipment.

These instructions do not purport to cover all details or variations in equipment, nor to provide for every possible contingency to be met during installation, operation, and maintenance. The contents of this publication are presented for informational purposes only, and while every effort has been made to ensure their accuracy, they are not to be construed as warranties or guarantees, expressed or implied, regarding the products or services described herein, their use or applicability, or any other information included herein. Changes, modifications, and/or improvements to equipment and specifications are made periodically and these changes may or may not be reflected herein. It is understood that Emerson may make changes, modifications, or improvements to the equipment referenced herein or to the document itself at any time. This document is intended for trained personnel familiar with the Emerson products referenced herein.

Emerson may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not provide any license whatsoever to any of these patents.

Emerson provides the following document and the information included therein as-is and without warranty of any kind, expressed or implied, including but not limited to any implied statutory warranty of merchantability or fitness for particular purpose.

Section 1:Introduction

1.1 Getting Started

This Safety Manual provides information necessary to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing the VersaMax SafetyNet System. This manual provides necessary requirements for meeting the IEC 61508 or IEC 61511 functional safety standards.

The PACSystems VersaMax SafetyNet System (using VersaMax Safety Network Interface Unit and VersaMax SafetyNet IO) is intended for use as part of a programmable electronic system as defined by IEC 61508. It is suitable for safety functions up to Safety Integrity Level 2 (SIL2).

⚠ WARNING

Failure to follow the instructions provided in this document will render your system non-compliant with SIL2 certification.

The PACSystems VersaMax SafetyNet System employs a “1oo1D” (i.e., 1 out of 1 with diagnostics) architecture to achieve SIL2. IC695CPS400 controllers may be used in redundant mode to increase system availability, but this is neither required by, nor relevant to, the safety-related performance of the system.

Configuring and programming the PACSystems VersaMax SafetyNet System must be via an Emerson Automation Solutions software program known as the PAC machine Edition (PME).

In addition to completing the actions specifically related to the SafetyNet System, it is necessary to satisfy the wider requirements of IEC 61508. This includes such elements within the framework of the safety lifecycle, such as hazard and risk analysis and defining the safety requirements specification. This work must be carried out through appropriate and competent safety management procedures and staff.

Notes: This manual applies to RX3i IC695CPS400 controller, VersaMax Safety Network Interface Unit IC200SBI001, and VersaMax IO modules (IC200ALG264SN, IC200MDL650SN and IC200MDL750SN).

1.2 Installation and Commissioning

Refer to PACSystems GFK-2314 RX3i System User manual, GFK-1504 for SBI/IO modules, carriers, GFK-3301 IMR for VersaMax, GFK-3291 for CPS400 and third-party instruction/safety manuals for FTAs for installation details.

1.3 Terms

Items	Description
Safety	Freedom from unacceptable risk of harm
Functional Safey	The ability of a system to carry out the actions necessary to achieve or to maintain a defined safe state for the equipment, machinery, plant, apparatus under control of the system
Basic Safety	The equipment must be designed and manufactured such that it protects against risk of damage to persons by electrical shock and other hazards and against resulting fire and explosion. The protection must be effective under all conditions of the nominal operation and under single fault condition
Black Channel	In the Black Channel principle the communications safety layer is implemented in the components of the safety system itself. As per IEC-61508, the measures necessary to ensure the failure performance of the communication process shall be implemented in the E/E/PE safety-related subsystems or elements that interface with the communication channel in accordance with the IEC 61784-3 or IEC 62280 series as appropriate.
Safety Assessment	The investigation to arrive at a judgment - based on evidence - of the safety achieved by safety-related systems
Fail-Safe State	State where outputs are de-energized and PLC is in safe state without jeopardizing the process/environment.
Fail Safe	Failure that casues the PLC and and los to go to the defined fail-safe state without a demand from the process.
Fail Dangerous	Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by the safety system.
Fail Dangerous Detected	Failure that is dangerous but is detected by the safety system.

Fail Annunciation Undetected	Failure that does not cause a false trip or prevent the safety function but does cause loss of an automatic diagnostic and is not detected by another diagnostic.
Fail Annunciation Detected	Failure that does not cause a false trip or prevent the safety function but does cause loss of an automatic diagnostic or false diagnostic indication.
Fail No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function.
Industrial Ethernet	This refers to standard Ethernet protocol used in industrial environment for communication between different components of safety system. It is designed to withstand harsh conditions and ensure the reliable, secure, high speed and efficient transfer of data in industrial control systems.

Industrial Ethernet This refers to standard Ethernet protocol used in industrial environment for communication between different components of safety system. It is designed to withstand harsh conditions and ensure the reliable, secure, high speed and efficient transfer of data in industrial control systems.

Logic Solver The logic solver is the subsystem that executes the logic to take safety action. Its part of BPCS (Basic Process Control System) or SIS that performs one or more logic functions. Examples include electrical systems, electronic systems, programmable electronic systems, pneumatic systems, and hydraulic systems. Sensors and final elements are not part of the logic solver.

Low demand mode Mode, where the frequency of demands for operation made on a safety-related system is no greater than once per year and is no greater than twice the proof test frequency.

1.4 Abbreviations

Abbreviation	Description
EGD	Ethernet Global Data Protocol
FMEDA	Failure Modes, Effects and Diagnostic Analysis
FTA	Field terminal assembly
HFT	Hardware Fault Tolerance
I/O	Input/Output

Abbreviation	Description
MOC	Management of Change. These are specific procedures often done when performing any work activities in compliance with government regulatory authorities.
PFDavg	Average Probability of Failure on Demand
PME	PAC Machine Edition
SBI001	Safety Network Interface Unit
SFF	Safe Failure Fraction, the fraction of the overall failure rate of a device that results in either a safe fault or a diagnosed unsafe fault.
SIF	Safety Instrumented Function, a set of equipment intended to reduce the risk due to a specific hazard (a safety loop).
SIL	Safety Integrity Level, discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems where Safety Integrity Level 4 has the highest level of safety integrity and Safety Integrity Level 1 has the lowest.
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
1oo1D	One out of one with diagnostics - a system which has no hardware fault tolerance and some level of diagnostic coverage to detect faults.
1oo2	One out of two voting arrangement - a system which has a hardware fault tolerance of “one”

1.5 Related VersaMax Manuals

For more information about PACSystems VersaMax SafetyNet System components, consult the following manuals.

Titles	Description
GFK-1504, PACSystems™ VersaMax IO Modules, Power Supplies & Carriers User’s Manual	Describes the installation and operation of the PLC System. This manual also contains general information about CPU operation and program features.
GFK-3290, PACSystems™ VersaMax Safety Network Interface Unit IPI	Describes the installation and operation of the VersaMax Safety Network Interface Unit (IC200SBI001). The manual also contains basic features of VersaMax Safety Network Interface Unit.

GFK-2314, PACSystems™ RX3i System User Manual	Describes the installation and operation of the RX3i products. The manual also contains overview of various RX3i products and features.
GFK-2222, PACSystems™ RX3i and RSTi-EP CPU Reference Manual	Describes general information about PACSystems CPU operation and product features.
GFK-2224, PACSystems™ RX3i and RSTi-EP TCP/IP Ethernet Communications User Manual	Describes Ethernet interfaces for PACSystems family of controllers and also provide instructions for installing and applying the PACSystems Ethernet interfaces.
GFK-2950, PACSystems™ CPU Programmer's Reference Manual	Describes general information about programming a PACSystems CPU. It also provides detailed descriptions of specific programming requirements.
GFK-3279, VersaMax Function Block Manual	Describes the Safety C-blocks used for developing safety application.
GFK-3280, VersaMax Safety NIU Manual	Describes general information about VersaMax Safety NIU SBI001. It also provides information related to template to be used for safety system.
GFK-3296, PACSystems™ VersaMax SafetyNet CPS400/SBI001 Templates IPI	Provides overview of PME Templates and VersaMax SafetyNet ToolChest IPI
IEC 61508: 2010	Functional safety of electrical/electronic/ programmable electronic safety-related systems
ANSI/ISA 84.00.01-2004 (IEC 61511 Mod.)	Functional Safety – Safety Instrumented Systems for the Process Industry Sector

Section 2:VersaMax SafetyNet System Components

2.1 System Description

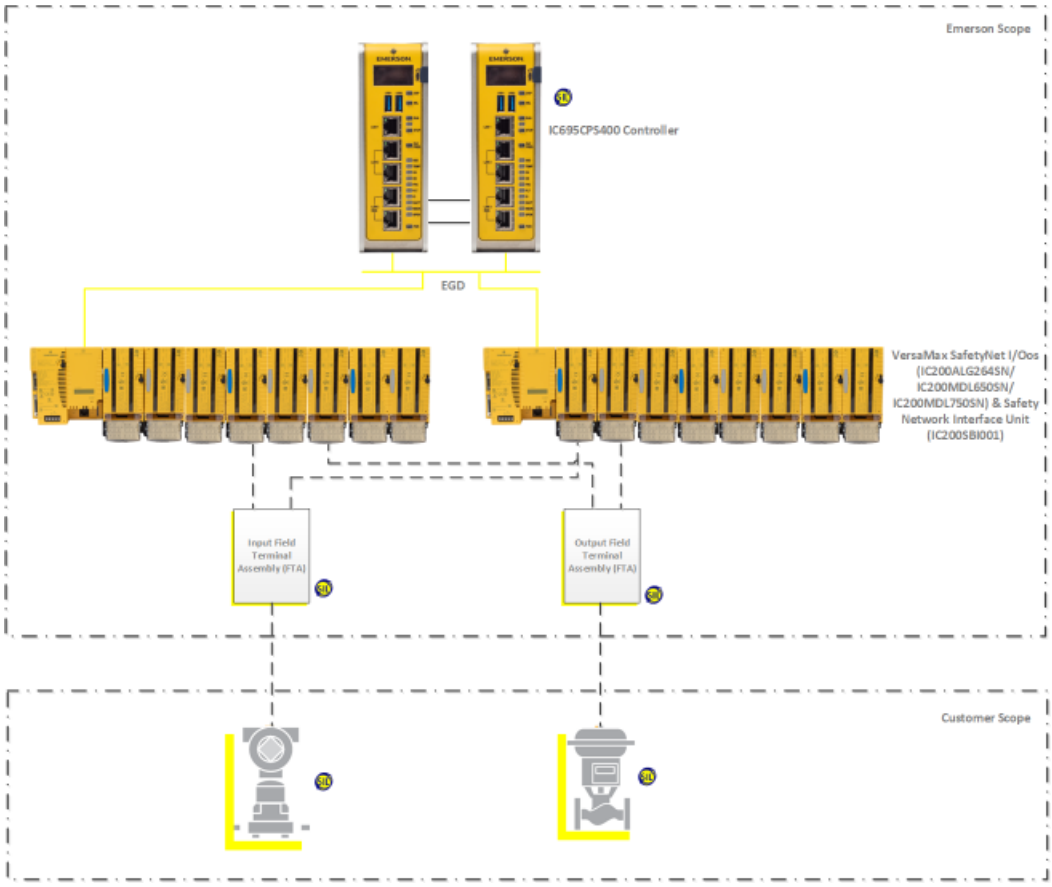
The PACSystems VersaMax SafetyNet System consists of the following components:

- One or twoRX3i Safety CPUs (IC695CPS400)
- RX3i Energy Pack for each RX3i Safety CPU (IC695ACC403SN)
- Two or more VersaMax SafetyNet Safety Network Interface units (IC200SBI001)
- VersaMax SafetyNet power supply for each VersaMax Safety Network Interface unit (IC200PWR002SN)
- VersaMax SafetyNet I/O carriers (IC200CHS022SN)
- VersaMax SafeytNet I/O modules (IC200ALG264SN, IC200MDL650SN and IC200MDL750SN)
- Field Terminal Assemblies (FTA) for connecting VersaMax I/O modules to safety sensors and actuators

The System also uses PAC Machine Edition (PME) software tool for configuration and programming purposes. The data required to establish the suitability of the PACSystems VersaMax SafetyNet System for safety-related applications is given in the data sheets for each of the components.

The figure below gives an overview of a PACSystems VersaMax SafetyNet System.

Figure 1: PACSystems VersaMax SafetyNet System Architecture



2.2 PACSystems VersaMax SafetyNet System Architecture

The default system architecture consists of a redundant IC695CPS400 controller in a Hot-Standby configuration. This configuration uses VersaMax I/O racks with a Safety Network Interface Unit and I/O modules, which use FTAs in 1oo2 scheme. Communication between VersaMax Safety Network Interface unit IC200SBI001 and the VersaMax I/O modules occurs via backplane. Communication between Safety Network Interface unit IC200SBI001 and IC695CPS400 controller takes place via an Industrial Ethernet network utilizing EGD protocol with Safety Black Channel communications. The Field terminal assemblies (FTAs) are used for splitting the input field signals to primary and secondary racks. The outputs from primary and secondary racks are wired to AND or OR type FTA depending on application requirement. For AND type FTA both the outputs from primary and secondary racks shall be energized for the field output to be energized. For

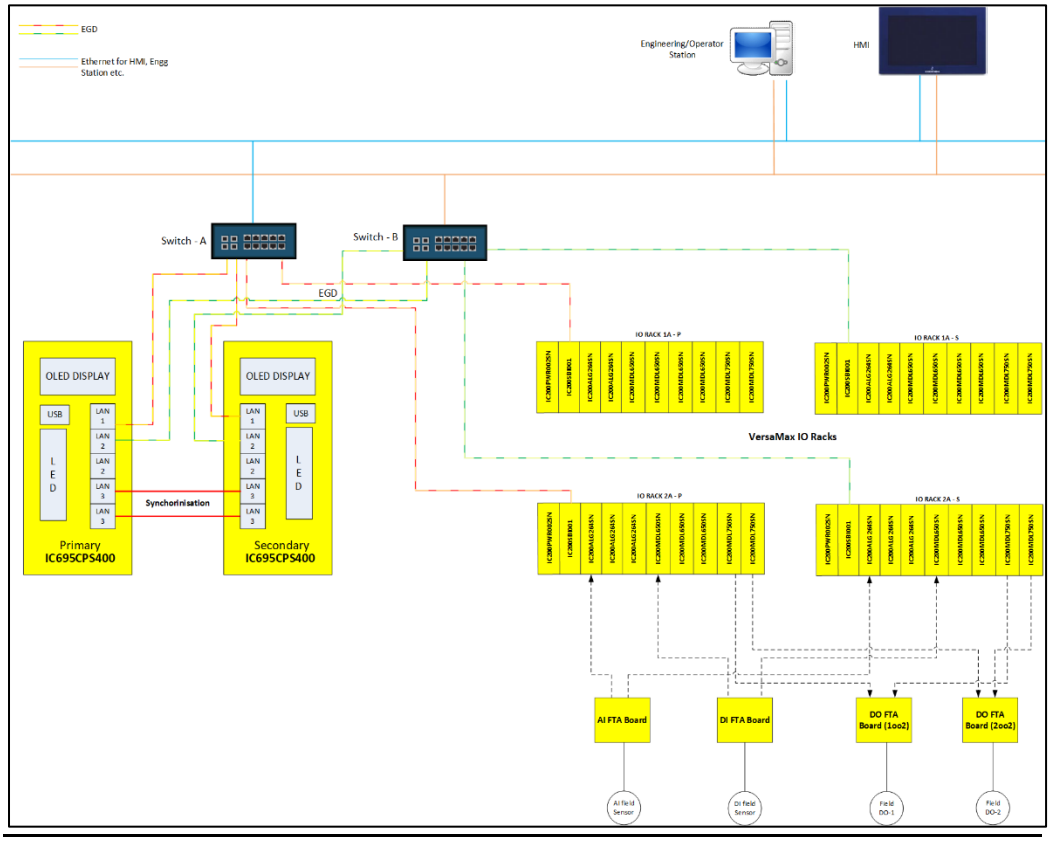
OR type FTA one of the outputs from primary and secondary racks shall be energized for the field output to be energized.

Field terminal assemblies (FTAs) are used to divide the input field signals to primary and secondary racks. The outputs from primary and secondary racks are connected to either an AND or OR type FTA, depending on application requirement. In the case of an AND type FTA, both the outputs from primary and secondary racks must be energized for the field output to be energized. For an OR type FTA, only one of the outputs from primary and secondary racks needs to be energized for the field output to be energized.

Notes: PACSystems™ RX3i IC695CPS400 safety controller can be used in simplex deployment also. In default architecture, it is installed in redundant pair for increased process availability.

Below architecture can be used in PACSystems VersaMax SafetyNet System using VersaMax I/O racks.

Figure 2: PACSystems VersaMax SafetyNet System Architecture



2.3 PACSystems VersaMax SafetyNet System Components

The table in this section lists components that may be used with SIL2 PACSystems VersaMax SafetyNet System.

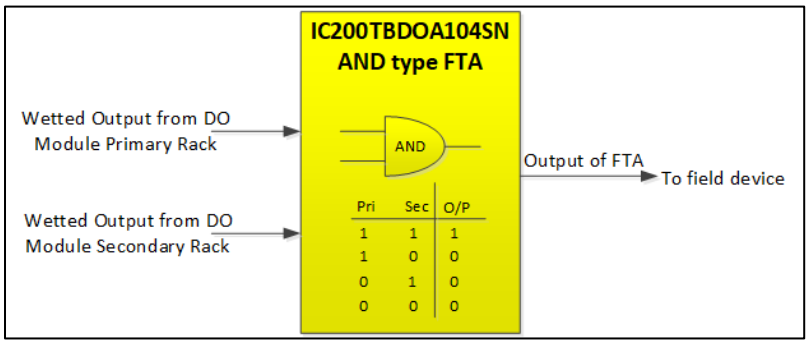
Device Type	Part Number	Description
Controller	IC695CPS400	PACSystems RX3i CPS400 controller
Energy Pack	IC695ACC403SN	Energy Pack for IC695CPS400 controller
I/O rack Power Supply	IC200PWR002SN	VersaMax I/O Rack Power Supply 24 VDC W/EXP 3.3VDC
I/O rack Carrier	IC200CHS022SN	VersaMax I/O module Carrier
Safety Network Interface unit	IC200SBI001	VersaMax Safety Network Interface unit (controls I/O within one rack and connects to Safety IC695CPS400 controller over EGD communication)
I/O module	IC200ALG264SN	VersaMax SafetyNet Analog Input Module
I/O module	IC200MDL650SN	VersaMax SafetyNet Discrete Input Module
I/O module	IC200MDL750SN	VersaMax SafetyNet Discrete Output Module
Field terminal assembly (FTA)	Third party	FTA AI Splitter for VersaMax SafetyNet Analog input
Field terminal assembly (FTA)	Third party	FTA DI Splitter for VersaMax SafetyNet Discrete input
Field terminal assembly (FTA)	Third party	FTA DO DTT 1oo2 for VersaMax SafetyNet Discrete output (AND Logic)
Field terminal assembly (FTA)	Third party	FTA DO ETT 1oo2 for VersaMax SafetyNet Discrete output (OR Logic)

2.4 PACSystems VersaMax SafetyNet System Normal and Safe States

The VersaMax SafetyNet Digital Output (DO) Module can provide digital outputs that can be used for both normally energized or normally de-energized applications.

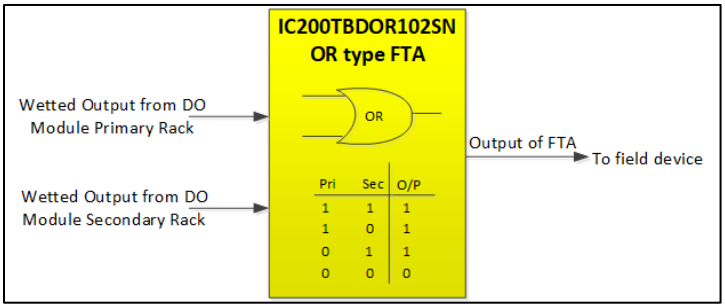
For normally energized applications, it is recommended to use a DO AND FTA. This involves wiring the output of both the Primary and Secondary VersaMax IO racks DO modules to an AND type FTA and then wiring the output of the FTA to the field device.

Figure 3: PACSystems VersaMax SafetyNet AND Type FTA Typical Diagram



It is recommended to use DO Oring FTA for applications that are normally de-energized. The DO module outputs of both the Primary and the Secondary VersaMax IO racks should be connected to an OR type FTA. The output of the FTA is then connected to the field device.

Figure 4: PACSystems VersaMax SafetyNet OR Type FTA Typical Diagram



For both normally energized and normally de-energized, the safe state is de-energized on detection of internal fault.

In case of normally energized outputs, they are de-energized to their safe state upon command or detection of an internal fault.

On the other hand, normally de-energized outputs are energized on command, for example, when opening the damper of a tunnel on fire detection. However, in case of an internal fault, the outputs will be held in the safe state of de-energized.

In the event of a of loss of power, the DO will fail to safe state which is de-energized.

Note: Users can utilize third party SIL2/SIL3 certified splitters and relays as a substitute for FTAs providing equivalent functionality

2.5 PACSystems™ RX3i IC695CPS400 controller

The PACSystems™ RX3i IC695CPS400 controller is a richly featured programmable controller equipped with built-in program memory. It can perform several functions, including but not limited to logic solving, I/O processing, event generation, timing/counting, communication, and more. The standalone CPU utilizes a multi-core microprocessor to running real-time deterministic control applications.

In the event that the IC695CPS400 controller detects a dangerous fault that could hinder the SafetyNet System's safety function), it initiates a controlled shutdown. The controlled shutdown serves two purposes – first, to ensure that the SafetyNet System enters failsafe mode (with outputs set to the safe state of de-energized); and second, to record sufficient data to allow the reason for the shutdown to be determined.

Only authorized users can change an IC695CPS400 controller's configuration and application programs.

2.5.1 IC695CPS400 controller Diagnostics Checks

The IC695CPS400 controller automatically carries out a number of diagnostic checks on a continuous basis. All checks are monitored and completed at least once every 15 minutes. This period is called the diagnostic test interval.

The internal, automatic diagnostic tests carried out by the PACSystems VersaMax SafetyNet System are sufficient to meet the requirements for use in SIL2 safety-related applications.

2.5.2 Redundant IC695CPS400 controllers

Hot Standby CPU Redundancy allows a critical application or process to continue operating should a failure occur in the active CPU. A Hot Standby system uses two CPUs: an *Active* unit that actively controls the process, and a *Backup* unit that is synchronized with the Active unit and can take over the process if it becomes necessary. The two units are synchronized when both are in Run Mode: The Backup unit will have received the latest status and synchronization information from the Active unit via a redundancy link, and each is running its logic solution in parallel.

IC695CPS400 controller use their own built-in LAN3 ports to support the required redundancy communications links between Active and Backup units. LAN3 is a dedicated, secure, point-to-point Ethernet link which does not support any additional equipment. Only a pair of CPS400 CPUs may be interconnected on LAN3. Control automatically switches to the Backup unit when a failure is detected in the Active unit. The system runs synchronously with a transfer of all control data that defines machine status and any internal data needed to keep the two CPUs operating in sync. Energy packs with IC695CPS400 controllers

shall be installed in PACSystems VersaMax SafetyNet System for redundant operation.

Critical control data plus all redundant outputs must be included in the output synchronization data transfer. The transfer of data from the Active unit to the Backup unit occurs twice per sweep, once before the logic is solved and once after the logic is solved. These CPU-to-CPU transfers are checked for data integrity.

Using IC695CPS400 controllers in redundant mode will increase their availability but will have no effect on their ability to perform a safety-related function. A PACSystems VersaMax SafetyNet System is certified for use as part of a SIL2 system, whether the controllers are used in simplex or redundant mode.

2.5.3 Downloading Safety Applications

When permitted (ensure that you are online in Programmer Mode to the target controller) new safety applications can be downloaded to IC695CPS400 controllers from the PME.

It is possible to download new applications online without interrupting the safety function with either simplex or redundant IC695CPS400 controllers. However, in the PACSystems VersaMax SafetyNet system, it is not permitted to make changes to safety system while it is running.

For each target that you download, Machine Edition performs a validation. Any errors that occur are displayed in the Build tab of the Feedback Zone. If there are no errors, Machine Edition builds and sends all the necessary run-time files to the controller.

Downloading a new safety application to redundant IC695CPS400 controllers is same as for simplex controllers. The new safety application is simultaneously downloaded to both active and standby controllers to ensure that they remain in the same state at all times.

2.5.4 Downloading New controller Firmware

When IC695CPS400 controller specific firmware is available (ensure that you are online in Programmer Mode to the target controller) new firmware can be downloaded to IC695CPS400 controllers from the controller Webpage. The new firmware zip file can be downloaded from Emerson Industrial automation controls support website. Refer to “Instructions for Web/HTTP Firmware Upgrade” document for step-by-step procedure to upgrade the firmware.

To carry out such a firmware upgrade the IC695CPS400 controller shall be in STOP mode.

⚠ WARNING

Do not perform firmware upgrade on IC695CPS400 controller unless informed by Emerson.

2.6 PACSystems VersaMax SafetyNet IO Modules

VersaMax SafetyNet modules perform additional software diagnostic checks and have hardware specifically designed for safety-related applications.

2.6.1 IO Module Configuration

VersaMax SafetyNet IO Modules are configured using PME.

When permitted and approved by local operating procedures, new IO Configuration can be downloaded to VersaMax SafetyNet IO Modules (via IC200SBI001), without interrupting the operation of other IO Modules mounted on the same node.

To carry out such download, the IC200SBI001 must first be in “Stop Mode”.

Refer to GFK-1504 PACSystems™ VersaMax SafetyNet IO Modules, Power Supplies & Carriers User’s manual for respective IO module wiring for proper operation.

2.6.2 LED Indication

Each VersaMax IO Module features a green OK LED marked “OK”, to indicate backplane power is present. For input and output IO module, individual green LEDs indicate the on/off state of each input/output point. LEDs may be on or off.

Refer to GFK-1504 PACSystems™ VersaMax SafetyNet IO Modules, Power Supplies & Carriers User's manual for detailed description of LED indicators for each module.

2.6.3 Module States

VersaMax SafetyNet IO Modules can be in one of two states as below.

- Running State – the IO module is working normally and reading inputs or writing outputs as required.
- Fault State – the IO module has been through a Shutdown, either because loss of backplane communication with IC200SBI001 or because a module hardware fault has been detected or if there is loss of field power.

Running State

This state is the normal operating state for the module. In this state:

Input channels are scanned and output channels are written to.

- Backplane communication is fully active, accepting all valid commands.
- Background diagnostics are running and if a failure is detected (Viz. Communication failure with IC200SBI001 or IC200SBI001 enters in fault state), then the module may enter fault state and by default outputs are de-energized.
- The individual green LEDs indicate the on/off state of each channel. (The individual channel green LEDs are available for only discrete input & output module only)

Fault State

The module will enter the Fault State either if IC200SBI001 in fault state or there is loss of backplane communication with IC200SBI001. In this state:

The OK LED blinks off.

- All channels are set to inactive (no scanning of inputs is performed, outputs are de-energized)
- Loss of module is indicated in the IO fault table. The module can only exit the Fault State by a power cycle or replacing the module. The addition of module is indicated in IO fault table.

⚠ WARNING

Care should be taken to replace IO module in a running plant. It is always recommended to perform IO module swapping offline.

2.6.4 VersaMax Analogue Input Module

The IC200ALG264SN VersaMax SafetyNet Analogue Input Module is a 15 channel module for use with 2-, 3- or 4-wire transmitters – which may, or may not, be HART devices. (Note that 3-wire transmitters may only be used which have a specified return current of no more than 25mA). The inputs are suitable for use in SIL2 applications, using a "1oo2" architecture to meet the requirements for use in a safety-related system.

Detailed information regarding the use of the VersaMax SafetyNet Analogue Input Module is given in the appropriate data sheets and user documentation. The information given here only relates to the safety-related aspects of the module.

For PACSystems VersaMax SafetyNet System, only 0-20mA input range shall be used.

Notes: HART data is not supported by IC200ALG264SN Analogue Input Module. If HART data is required on plant AMS system, then, HART multiplexers shall be used which will be end users' responsibility.

Configuration

Each module can be configured for 0-20mA with jumper installed. The analog inputs are software-configurable to either default or hold last state upon loss of module.

On power up, all VersaMax SafetyNet Analogue Input Module channels will be active after first scan cycle.

Under-range and Over-range Alarms

Input readings below 4mA and above 20mA detection can be performed via application logic in IC695CPS400 controller.

By configuring the VersaMax SafetyNet Analogue input module, 0-20mA, logically the Under range & over range alarms can be generated based on the count reading. For 20mA the count is 32000 and for 4mA the count is 6400. For 3.4mA count is 5440, if the count is <5440 the signal can be declared as under range and for over range, if the reading is 20.383mA the count is 32616 and above 20.384mA count goes into fixed value 32767, which can be then declared as over-range.

VersaMax SafetyNet analogue input module IC200ALG264SN shall be configured for 0-20mA, open wire fault can be generated if the input current is <3.4mA.

Analogue Input Diagnostics

The VersaMax SafetyNet Analogue Input Module reports a Loss of Internal Power fault for field-side circuits. The module reports an Open Wire fault for

each channel, when in 4-20mA mode or in 0-20mA (through application logic).

Intrinsically Safe Analogue Inputs

If an intrinsically safe field connection is required, an external barrier (that meets both the hazardous area and functional safety requirements) should be used.

2.6.5 VersaMax Digital Input Module

The IC200MDL650SN VersaMax SafetyNet Discrete Input Module is a 32-channel module, with four discrete groups of 8 input each. Inputs in each group can be either positive logic inputs that receive current from input devices and return the current on the common, or negative-logic inputs that receive current from the common and return current to the input device. Input devices are connected between the input terminals and common terminals.

When configured as an input, the channel is suitable for use in SIL2 safety functions. The architecture is “1oo2”. In PACSystems VersaMax SafetyNet System both the inputs from primary and secondary rack shall be configured as positive logic.

Detailed information regarding the use of the VersaMax SafetyNet Discrete input Module is given in the appropriate data sheets and user documentation. The information given here only refers to the safety-related aspects of the module.

Configuration

A VersaMax SafetyNet discrete input module basic input on/off response time is 0.5ms. Based on application there is provision of adding the filter time to compensate conditions such as noise spikes or switch bounce etc. The default filter time should be configured as 1ms.

The discrete inputs are software-configurable to either default or hold last state upon loss of module. A VersaMax SafetyNet discrete input module shall be configured as “Default” i.e. de-energized in module parameters in case of loss of module.

On power up, all VersaMax SafetyNet Discrete Input Module channels will be active after first scan cycle.

2.6.6 VersaMax Digital Output Module

The IC200MDL750SN VersaMax SafetyNet Discrete Output Module is a 32-channel module, with two discrete groups of 16 outputs each. The outputs are positive or sourcing type outputs. They switch the loads to the positive side of the DC supply and thus supply current to the loads.

Configuration

The discrete outputs are software-configurable to either default or hold last state upon loss of module. A VersaMax SafetyNet Discrete output module shall be configured as “Default” i.e. de-energized in module parameters in case of loss of module.

On power up, all VersaMax SafetyNet Discrete Output Module channels will be active after first scan cycle.

Intrinsically Safe Discrete Inputs and Outputs

If an intrinsically safe field connection is required, an external barrier/relay (that meets both the hazardous area and functional safety requirements) should be used.

2.7 VersaMax Safety Network Interface Unit (IC200SBI001)

The Safety Network Interface unit acts as controller for a set of safety I/O modules. Power for module operation is provided by a power supply that installs directly on the SBI. It is interfacing device between IC695CPS400 controller and VersaMax SafetyNet I/O modules. It transmits data between IC695CPS400 and VersaMax SafetyNet I/O modules back and forth using Black Channel safety communications approach transmitted over EGD protocol. The VersaMax SafetyNet IC200SBI001, I/O module and EGD configuration is performed via PME.

If the IC200SBI001 goes to fault (i.e., one that would prevent the PACSystems VersaMax SafetyNet System from carrying out its safety function) then it will initiate a shutdown. A shutdown has two objectives – firstly, to ensure that the PACSystems VersaMax SafetyNet System enters its failsafe mode (with outputs set to the safe state of de-energized); and secondly, to record sufficient data to allow the reason for the shutdown to be determined.

Only authorized users can change a IC200SBI001 configuration and I/O configuration.

The VersaMax Safety IC200SBI001 is suitable for use in SIL2 applications, using a “1oo2” architecture to meet the requirements for use in a safety-related system.

2.7.1 VersaMax Safety Network Interface unit IC200SBI001 Diagnostics Checks

The VersaMax Safety Network Interface unit (IC200SBI001) module automatically carries out a number of diagnostic checks on a continuous basis.

The internal, automatic diagnostic tests carried out by the PACSystems VersaMax SafetyNet System are sufficient to meet the requirements for use in SIL2 safety-related applications.

2.7.2 Downloading EGD and IO configuration

When permitted, a new I/O / EGD configuration can be downloaded to IC200SBI001 from PME.

It is not possible to download new configurations online without interrupting the safety function. Additionally, online downloads to EGD configuration are not permitted.

Validation checks are performed by PME before downloading any configuration in IC200SBI001.

2.7.3 Downloading New IC200SBI001 Firmware

When permitted, a new firmware can be downloaded to IC200SBI001 using a serial port on IC200SBI001.

Online (i.e. when plant is running) download of firmware to IC200SBI001 is not possible hence it should be carried out in Offline mode only.

The new firmware zip file can be downloaded from Emerson Industrial automation controls support website. Refer to “Instructions for Upgrading” document for step-by-step procedure to upgrade the firmware.

To carry out such an off-line download, the IC200SBI001 must first be in “Stop Mode”.

⚠ WARNING

Do not perform firmware upgrade on IC200SBI001 Safety Network interface module unless informed by Emerson.

2.8 Redundant Power Supplies

The PACSystems VersaMax SafetyNet System is designed to be used with any third-party power supplies to provide the 24 Vdc "Bussed Field Power" from AC mains supplies.

Redundant power supplies can be implemented by “pairing” supplies. While this is not required for the certified safety integrity level, it can enhance system availability.

The power supplies shall incorporate protection against faults which could cause the output voltage to increase, which could in turn lead to a dangerous failure in the VersaMax SafetyNet System.

The PACSystems VersaMax SafetyNet System also uses IC200PWR002SN 24VDC power supply mounted in each rack which provides backplane power for CPU & IO modules in that particular rack. IC200PWR002SN power supply incorporates protection against short circuit, overload and reverse polarity.

The dangerous undetected failure rates provided for each VersaMax rack component assume that the IC200PWR002SN power supply is used, in which case no additional failure allowance is necessary. When designing de-energize-to-trip systems, the power supply is not critical to safety because all failures are considered safe. For energize-to-trip systems, the independent monitored power source is recommended.

For further information regarding the provision of power supply for installation, grounding, refer to Chapter two of the PACSystems™ VersaMax SafetyNet I/O Modules, Power Supplies & Carriers User's manual (GFK-1504).

2.9 Field Terminal Assembly (FTA)

The PACSystems VersaMax SafetyNet System uses FTAs to connect field sensors to primary and secondary VersaMax I/O racks. The FTAs essentially act like splitter to provide inputs to VersaMax SafetyNet I/O racks and for outputs they act like voters.

FTAs only require wiring and do not need any software configuration. The PACSystems VersaMax SafetyNet System uses four types of FTAs: Analogue input , Discrete input, Discrete output – AND outputs, and Discrete output – ORed outputs. For further details on FTAs refer to the respective third-party suppliers product documentation and safety manual.

2.10 PAC Machine Edition (PME)

PAC Machine Edition offers a complete solution for the development of automation applications, in one package. Machine Edition features an integrated development environment and tools that enable user for building applications/projects that will be downloaded to IC695CPS400 controller. PME can be used with both non-safety and/or VersaMax SafetyNet Systems with ProPlus development suite product only.

This section describes the features of the PME applicable to the PACSystems VersaMax SafetyNet System – more general information regarding the operation and use of the PME can be found in the PAC Machine Edition Logic Developer – PLC Getting Started Guide (GFK-1918).

A summary of PME features specific to its use with VersaMax SafetyNet Systems is given below;

Two modes of operation in Online mode i.e., Monitor mode and Programmer mode

- Password protection along with various privilege levels of security access to control which personnel are allowed to perform operations related to the safety.
- Program blocks can also be password protected, to control access to safety-related program blocks.

The various privilege levels are also utilized to restrict external writes into VersaMax SafetyNet System.

- A Validation tool is included in PME which displays error messages in feedback zone before downloading to controller.

PAC Change Management Tool for Change control log and Version management

2.10.1 Monitor Mode and Programmer Mode

When online in monitor mode, users can monitor the controller while it is executing. Logic cannot be edited on their computer or the controller. Users cannot change any values on the controller. Depending on level of access to the controller and Change Management permission levels, users can upload from the controller.

This is the normal, running state of the VersaMax SafetyNet System.

When online in Programmer Mode, users can make changes on their computer and the controller and can monitor the controller while it is executing. Users can edit any type of controller logic on their computer. Depending on user level of access to the controller and Change Management permission levels, user can:

- Upload from the controller
- Control the controller while it is executing
- Control any change values on the controller
- Download to the controller

Instructing the PACSystems VersaMax SafetyNet System to leave Monitor Mode and enter Programmer mode – allows the user to make modifications to configuration parameters or logic changes, during which time the safety function can still operate.

Programmer Mode can only be entered when a user designated as having safety responsibility enters the appropriate password.

If the controller is running, users can download only logic that is not equal to the controller's current logic and the Download to controller dialog box does not appear.

When offline from a PACSystems, there is no ongoing communication between the controller and the development computer. A physical communication link is not required as long as users only edit logic; it is required only when users want

to communicate with the controller. The only controller operations users can perform while offline are to go online.

2.10.2 Password/Privilege levels Protection

IC695CPS400 controller is equipped with password management. Passwords are disabled by default, but can be enabled, disabled, or configured with PAC Machine Edition (PME). When in Online mode, PLCs can be password protected at varying privilege levels (1-4).

There are four different privilege levels. Level 1 provides the least access and Level 4 provides the most access. The current privilege level is identified by the padlock icon on bottom row of PME screen.

Users with Safety Responsibility can be assigned appropriate privilege levels. This will allow them access to IC695CPS400 controller various configuration and programming options. Users with Safety Responsibility should use these passwords and privilege levels in a VersaMax SafetyNet System.

The program blocks in which safety logic is configured should be password protected to control access to these blocks.

The external writes from HMI or third-party system can also be restricted by using various privilege levels. Note that when writes are sent via Ethernet, the communication must be via the OPC UA Server.

Refer to PACSystems™ RX3i and RSTi-EP CPU Reference Manual (GFK-2222) for more information on the PLC operation restrictions in each privilege level and also password protection.

2.10.3 SafetyNet Logic Validation Tool

Safety application programs must be validated before they can be downloaded to the IC695CPS400 controller. Validating your target detects syntax and configuration errors on the target. Error messages are generated for each error and displayed in the Feedback Zone in PME.

The user may decide when to run the tool, but it will not be possible to download a target to a IC695CPS400 controller that has not passed static analysis (validation).

Section 3:Maintenance Overrides

Maintenance overrides allow sensors and actuators to be proof tested and/or maintained, by temporarily suppressing the normal operation of a safety function. The requirements for maintenance overrides must be considered during the specification and design of the safety system – and the implementation must be tested as rigorously as the other elements of the system during acceptance testing.

The maintenance override facility may also be used to meet other requirements – for example to force a system shut-down or to re-start the safety system after a shut-down has taken place and to reset channels that have entered failsafe due to faults, once the fault has been cleared.

An example would be using a maintenance override to disable a specific part of the safety logic or to set a particular analogue input to a specific value.

Generally, maintenance overrides are initiated by remote communication with the controller. The remote communication – for example – would be from an HMI or DCS.

When an override is in place, the safety system is not providing the level of protection that it would normally provide. Hence, only authorized, specially trained personnel (operators) can change the parameters in safety-related systems via HMIs.

The operator who makes changes in a safety-related system via an HMI is responsible for the effect of those changes on the safety function.

Users must use a clear, comprehensive, and explicit operator procedure to make safety-related changes via an HMI.

The controller used to provide the safety function must accept the remote communication initiated by the HMI or DCS and take appropriate action to implement the maintenance override. This Safety Manual therefore gives particular attention to the management of this option of initiation of maintenance override via remote communication (from HMI or DCS) with the SafetyNet System.

Since the communication between HMI or DCS and PACSystems IC695CPS400 Safety controller is not SIL compliant, the restrictions such as use of privilege levels and use of OPC UA for maintenance override sent via Ethernet must be followed.

The maintenance override function must be written in to the SafetyNet application and tested and approved as an integral part of the application.

There is no limit to the number of maintenance override functions that can be incorporated into a particular SafetyNet application.

3.1.1 Activating a Maintenance Override by remote communication

A IC695CPS400 controller operating in “monitor” mode can accept a maintenance override instruction transmitted by remote communication from a host – such as an HMI or a DCS – subject to the following conditions:

- External writes are allowed on IC695CPS400 controller via privilege levels (this is mainly for Modbus communication) and for OPC-UA communication for HMI writes it can be controlled via HMI user management
- The tags to be used are defined in the controller’s external mapping table to allow writes from external sources
- Once the maintenance override is implemented, the IC695CPS400 password protection or HMI password protection should be again placed to prevent further access to the IC695CPS400 controller (any existing overrides remain in place, until the password protection is on, and they are removed by the appropriate instructions). While the maintenance override is active, the safety function (or functions) that is (or are) affected, will no longer be operating normally.
- Further maintenance override instructions may be sent and – if they satisfy the above requirements, they will be accepted in addition to any maintenance override instructions that are already in place.

3.1.2 Removing a Maintenance Override by Remote Communication

Removing the maintenance override by remote communication with a host such as an HMI or a DCS is the reverse of the process for setting.

A IC695CPS400 controller operating in “monitor” mode can accept an instruction to remove a maintenance override transmitted by remote communication from a host – such as an HMI or a DCS – subject to the following conditions:

- External writes are allowed on IC695CPS400 controller via privilege levels (this is mainly for Modbus communication) and for OPC-UA communication for HMI writes it can be controlled via HMI user management
- the tags to be used are defined in the controller’s external mapping table to allow writes from external sources
- Once the maintenance override is removed, the IC695CPS400 password protection or HMI password protection should be again placed to prevent further access to the IC695CPS400 controller.
- It is often useful to confirm that the safety function that has been subject to the maintenance override does not immediately trip once the override is

- removed. It is recommended that actual input values shall be verified by the operator before removing the particular override.

3.2 Removing a Maintenance Override Using SafetyNet Inputs

- By preference, maintenance overrides should be removed by a switch connected to a VersaMax SafetyNet Digital Input channel – normally set manually by an operator. Different switches can be used to clear particular overrides and/or a switch could be used to clear all overrides from a particular IC695CPS400 controller.
- The use of such a switch would satisfy the requirement that there should be an "alternative" method of clearing the maintenance override, other than via remote communication.

⚠ WARNING

The application could automatically remove the maintenance override, perhaps after a given time period, but experience has shown that removing them in this way is neither a practical nor a safe approach.

Notes: if a function is required that will "clear all overrides" this can simply be implemented by writing the application so that setting a particular input (perhaps by operating a dedicated push-button) clears all maintenance overrides.

3.3 Recording Maintenance Override Activity

It is recommended to record maintenance override details, including the identity of the person who initiated the override, the time it occurred, the specific override initiated, and the time it was removed. Ideally, this information should be documented electronically. The PACSystems VersaMax SafetyNet System does not support this recording, and if electronic recording is to be implemented, it should be carried out within the host HMI or DCS.

3.4 Additional Measures When Using Maintenance Overrides

The following measures must or should be adopted during maintenance override:

- The duration of a given override shall be limited to the length of one operator shift (normally 8 hours), unless hardwired lamps/indicators are provided on the operator console.

- A loss of communication between the HMI or DCS host and the IC695CPS400 controller, where the maintenance override is initiated, must be clearly indicated to both the operator and maintenance engineer. This should be implemented on the HMI or DCS.

3.5 Resetting a Tripped Safety Function

Once the reason for the trip has been removed, the safety function can be reset prior to being brought back online. The feature/procedure similar to maintenance override can be useful in resetting a tripped safety function.

Section 4:Designing a Safety Instrumented Function (SIF) Using a Customer Product

4.1 Safety Function

The PACSystems VersaMax SafetyNet System is part of Safety function up to Safety Integrity Level 2 (SIL2). It can be used only in low demand applications such as: Emergency Shutdown System (ESD), Fire and Gas System (FGS) and infrastructure applications such as Ventilation system and Environmental control system with either de-energize-to-trip and energize-to-trip applications. The PACSystems VersaMax SafetyNet subsystem have been certified for fire and gas detection system and burner management systems from Exida according to relevant requirements of NFPA 72 (fire & gas) and NFPA 85, NFPA 86 and NFPA 87 (burner management). In case of fault the input/output will be set to zero state, which is fail-safe condition.

In all cases, the process safety time must be greater than the response time of the safety function (i.e. the response time of the VersaMax SafetyNet System, together with the response times of the sensors and actuators involved in the particular safety function).

The PACSystems VersaMax SafetyNet System is intended to be part of Logic Solver subsystem as defined per IEC 61508 and the achieved SIL level of the designed function must be verified by the designer.

4.2 Environmental Limits

The designer of a SIF must check that the product is rated for use within the expected environmental limits. For details on the environmental limits of the components of a PACSystems VersaMax SafetyNet, please refer to the PACSystems RX3i Systems Manual (GFK-2314) and PACSystems GFK-1504 manuals for various components of the System for environmental limits.

4.3 Application Limits

PME configuration and programming tool ensures that application limits are not exceeded for VersaMax SafetyNet System. For application limits, it is recommended that users refer to CPU Programmers Reference Manual (GFK-2950). VersaMax SafetyNet I/O Modules are configured using PME.

When permitted and approved by local operating procedures, new I/O Configuration can be downloaded to IC200SBI001.

4.4 Design Verification

A detailed Failure Mode, Effects, and Diagnostics Analysis (FMEDA) report is available from Emerson. This report details all failure rates and failure modes as well as the expected lifetime for various components in the PACSystems VersaMax SafetyNet System.

The achieved Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) design must be verified by the designer via a calculation of PFDAVG considering architecture, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

Notes: The exida exSILentia® tool is recommended for this purpose as it contains accurate models for the components and their failure rates.

When using the PACSystems VersaMax SafetyNet System in a redundant configuration, a common cause factor of at least 2% should be included in safety integrity calculations.

The failure rate data listed the FMEDA report is only valid for the useful lifetime of a VersaMax SafetyNet System. The failure rates will increase sometime after this time period. Reliability calculations based on the data listed in the FMEDA report for mission times beyond the lifetime may yield results that are too optimistic, i.e. the calculated Safety Integrity Level will not be achieved.

4.5 SIL Capability

4.5.1 Systematic Integrity

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 2. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer. A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than the statement without “prior use” justification by end user or diverse technology redundancy in the design.

4.5.2 Random Integrity

The product is a Type B Device. Therefore, based on the Diagnostic Coverage greater than 60% (SFF>90%), when it is used as the only component in a Logic Solver subsystem, a design can meet SIL 2 @ HFT=0.

4.5.3 Safety Parameters

For detailed failure rate information refer to the Failure Modes, Effects and Diagnostic Analysis Report for the VersaMax SafetyNet System.

4.6 Response Time

The response time for a particular SIF shall be less than the process safety time. The PACSystems VersaMax SafetyNet System has a maximum response time as a function of CPS400 controller and SBI001 sweep time. The PACSystems VersaMax SafetyNet System will have a maximum response time of 500ms. The actual response time will vary with each installation and depend on the complexity of the SafetyNet Logic program as well as the sweep time of IC695CPS400 controller.

The maximum response time is based on a DI initiating the trip to a DO.

Note following items concerning response time:

- The VersaMax SafetyNet side EGD produce time is constant at 10ms and on IC695CPS400 side EGD produce time follows sweep time.
- If application logic includes delays such as the trip delay time in voter function blocks, the response time will increase by the length of those delays.
- In addition to the response time of the VersaMax SafetyNet System, the response time of the input sensors and output actuators must be included for calculation of total SIF response time.
- Total worst-case time under normal conditions without any additional delays is 2*CPS400 Sweep time + 4*SBI001 Sweep time.
- For applications using redundant CPS400 controllers, although the probability of demand being present at the time of controller switchover is extremely low, it is recommended to assume additional overhead of 220ms in response time for particular sweep in situations necessary.

4.7 General Requirements and Competence

All SIS components including the PACSystems VersaMax SafetyNet System must be operational before process start-up.

User shall verify that the PACSystems VersaMax SafetyNet System is suitable for use in safety applications by confirming the PACSystems VersaMax SafetyNet System suitability.

Results from the proof tests shall be recorded and reviewed periodically.

Personnel performing maintenance and testing on the PACSystems VersaMax SafetyNet System shall be competent to do so.

Competence of Persons – Engineering

All persons involved in the initial implementation or modification of the application software should have appropriate training. Opportunities for training include reading product manuals, PME help (Companion) and attending a training class lead by Emerson experienced personnel. Formal training is

available through Emerson Educational Services. For information, visit: www.emerson.com/education

Competence of Persons - Installation and Hardware Maintenance

All persons involved in installation and hardware maintenance activities should have appropriate training. Opportunities for training include reading various Product manuals and attending a training class lead by Emerson experienced personnel. Formal training is available through Emerson Educational Services.

Competence of Persons – General

All persons involved in any aspect of VersaMax SafetyNet System, including engineers, operators, supervisors, maintenance personnel, and system administrators, should have training in the importance of safety instrumented systems. All persons should have specific training in the procedures for which they are responsible. The PACSystems VersaMax SafetyNet System administrators should ensure that all individuals having security passwords for PACSystems VersaMax SafetyNet System activities are trained and competent.

Section 5:Operations and Maintenance

5.1 Variable Health

The PACSystems VersaMax SafetyNet System detects VersaMax Safety network interface module failures, EGD communication failures and generates alarms as appropriate. The application code can be alerted to this type of failure by monitoring the health of the input variables using the AI_VOTING and DI_VOTING function blocks.

5.2 Proof Test Without Automatic Testing

The objective of proof testing is to detect failures within the PACSystems VersaMax SafetyNet System that are not detected by any automatic diagnostics of the system. The primary concern is undetected failures that prevent the safety instrumented function from performing its intended function.

The frequency of proof testing, or the proof test interval, is to be determined in reliability calculations for the safety instrumented functions for which a PACSystems VersaMax SafetyNet System is applied. The proof tests must be performed more frequently than or as frequently as specified in the calculation in order to maintain the required safety integrity of the safety instrumented function.

The results of the proof test should be recorded and any failures that are detected and that compromise functional safety should be reported to Emerson Automation Solutions. The proof test interval for the PACSystems VersaMax SafetyNet System operating in low demand mode will normally be between one and five years, depending on the application. Taking the IC695CPS400 PACSystems Safety controller, IC200SBI001 & VersaMax SafetyNet I/O modules through a power cycle i.e., turning the power OFF and back ON (this checks the correct operation of the hardware watchdogs, which can only be tested at start-up) is one way of performing proof test. No special tools are required for performing the offline proof testing. However, ensure all equipment have valid calibrations and record their make, model, serial numbers in test records.

The person(s) performing the proof test of a PACSystems VersaMax SafetyNet System should be trained in SIS operations, including bypass procedures, system maintenance and company Management of Change procedures. Every time before performing proof test ensure that there are no diagnostics alarms are present and bypass the safety loop or take any alternative measure to avoid the false trip.

The proof test for each module can also be performed as mentioned below. Refer to FMEDA report Appendix B for the Proof test coverage provided by below tests.

5.2.1 IC695CPS400 RX3i CPU Test Procedure

- Power cycle or perform the hard reset on the IC695CPS400 module to totally restart all complex devices at hardware level initialization.

5.2.2 IC200PWR002SN Power Supply Test Procedure

- Measure the actual 3.3V and 5V power output DC value and AC ripple and verify it is within manufacturer specified ranges.

5.2.3 IC200SBI001 Safety Network Interface Unit Test Procedure

- Power cycle or perform the hard reset on the IC200SBI001 module to totally restart all complex devices at hardware level initialization.
- Monitor/control results of all the other I/O module Proof tests from the IC695CPS400 controller.
- Verify both Safety Network Interface units provide same results.

5.2.4 IC200ALG264SN Analogue Input Module and its FTA AI Splitter Test Procedure

- Test each safety input channel by injecting test levels at the input to the FTA AI splitter module one at a time and monitoring the results through the IC695CPS400 safety controller using the following four voltage points as guidance:
  - below scale lower than 3.6 mA
  - low end in scale around 5 mA
  - high end in scale around 19 mA
  - above scale greater than 21 mA
- Verify proper value seen at the high-level safety controller and that values above and below scale are detected and indicated by out of normal range diagnostics and that there is agreement between the values from each of the redundant AI paths as seen by the CPS400 controller through the Rack IO Processor path.
- Inject a condition to create a difference between the redundant AI Inputs and verify proper voting/comparison actions by the CPS400 controller.

5.2.5 IC200MDL650SN Digital Input Module and its FTA DI Splitter Test Procedure

- Inject a de-energized state to the input of the FTA DI Splitter for each safety input one at a time and verify results through the CPS400 safety controller

that both redundant DI paths detect the change and proper action is taken for this condition.

- Inject a de-energized state to the input of the DI Module to each safety input one at a time to one of the two redundant DI modules and verify results through the CPS400 safety controller that the impacted path detects the change and the 1oo2 voter indicates a de-energized state.
- Repeat step 2 above from the other redundant DI Module.

5.2.6 IC200MDL750SN Digital Output Module and its FTA DO Voter Test Procedure

- Use the IC695CPS400 controller to directly control DO Module outputs for one of the two DO Modules one channel at a time forcing each channel energized and then de-energized while the other DO module has all outputs forced energized and verify the expected output at both the direct DO module outputs and the output of the FTA DO voter.
- Repeat step 1 swapping with DO rack has all outputs energized and which is forces energized and de-energized one channel at a time and again verify expected results at both the direct DO outputs and the output of the FTA DO voter.
- Lower the voltage to the external field power input to each DO Module and verify this condition is properly detected and acted upon by the DO Module and indicated at the IC695CPS400 controller.

5.3 Fail-Safe System

A system configuration where a fault anywhere in the safety system results in a system shutdown, that is, the system fails-to-safe state. In the fail-safe system, if a fault occurs anywhere in the system (that is, in the main controller, communications, safety interface module or I/O) it results in an Emergency Shutdown (ESD).

Below are some major scenarios in which VersaMax SafetyNet system will go to fail-safe state depending on in which portion of system fault has occurred.

Device	Failsafe condition
IC695CPS400	Both the IC695CPS400 controllers are power down
	Both the IC695CPS400 controllers are stopped from PME/OLED Display
	Both the IC695CPS400 controllers are stop faulted/restarted due to some fault
	EGD communication failure to the IC695CPS400 in Simplex architectures or to both IC695CPS400 controllers in High Availability architectures
	All LANs on the IC695CPS400 controller are disconnected

Device	Failsafe condition
IC200SBI001	VersaMax SafetyNet Primary/Secondary SBI module in Rack is power down
	VersaMax SafetyNet both SBI modules in Racks are power down
	VersaMax SafetyNet Primary rack LAN disconnected
	VersaMax SafetyNet Secondary rack LAN disconnected
	VersaMax SafetyNet Primary IC200SBI001 Stopped from PME
	VersaMax SafetyNet Secondary IC200SBI001 Stopped from PME
	VersaMax SafetyNet Primary rack IC200SBI001 Stop Fault
	VersaMax SafetyNet Secondary rack IC200SBI001 Stop Fault
	VersaMax SafetyNet Primary/Secondary rack I/O module failed
	Remove field power from VersaMax SafetyNet Primary rack I/O
	Remove field power from VersaMax SafetyNet Secondary rack I/O
	Loss of VersaMax AI/DI module
	Loss of VersaMax DO module
	FTA failed
	EGD communication failure to the IC695CPS400 in Simplex architectures or to both IC695CPS400 controllers in High Availability architectures

Note: In case of VersaMax I/O rack the fault in particular rack will affect the I/Os in that rack only.

5.4 Repair and replacement

Repairing a defective PACSystems VersaMax SafetyNet System (for example, controller, Safety Network Interface unit, or I/O modules) only consists of replacing the component. No special tools are required.

Refer to PACSystems™ RX3i Hot Standby CPU Redundancy User Manual (GFK-2308) and PACSystems™ RX3i and RSTi-EP TCP/IP Ethernet Communications User Manual (GFK-2224) for IC695CPS400 information such as how to evaluate and respond when faults, errors, or other conditions are annunciated. Refer to GFK-3291 for IC695CPS400 installation and maintenance requirements. For VersaMax IC200SBI001 refer to GFK-3280 PACSystems™ VersaMax Safety NIU Manual for faults, errors. Refer to GFK-1504 PACSystems™ VersaMax SafetyNet I/O Modules, Power Supplies & Carriers User Manual for installation. In order to report errors or product issues refer to Technical support Guide (GFK-3020).

5.5 Useful Life

The useful life of the PACSystems VersaMax SafetyNet System is discussed in the Failure Modes, Effects and Diagnostic Analysis Report.

5.6 Manufacture Notification

Any failures that are detected and that compromise functional safety should be reported to Emerson. Please contact Emerson customer service.

Section 6:General Application Requirements

6.1 Operator Interface

The PACSystems VersaMax SafetyNet System will normally be connected to operator interfaces made up of a combination of PC consoles (SCADA or PME), matrix panels, mimic panels etc.

These interfaces allow the operator to monitor the operation of the system and to override the automatic system in some instances (such as to prevent extinguishant release or to manually initiate alarms).

The PACSystems VersaMax SafetyNet System will allow detected faults (from line fault monitoring, internal System diagnostics etc.) to be displayed or indicated via the chosen Operator Interfaces according to the application program.

Loss of communication between the HMI and the PACSystems VersaMax SafetyNet System should be alarmed in the HMI – for example by a watchdog timer that would detect such a communication loss.

The operator interface can initiate maintenance override functions, but use of this capability is restricted – see Section 3.

6.2 Programming Interface

Programming, downloading safety-related parameters and application programs and switching between operating states is carried out from an engineering workstation running the PME & I/O configurator utility.

Access to the Programming Interface shall only be permitted for authorized and suitably qualified personnel. Access must be restricted by the use of passwords (and the options to do this are provided for within the PME) and/or some other forms of restricting access, such as safety management procedures or locks and restricted access keys.

The Programming Interface may also be used as the Operator Interface, but its use as a Programming Interface must be restricted as described above.

Programming may be carried out while the safety system is performing a safety function, but the system will not be SIL 2 compliant (i.e. the system is not in Monitor Mode, it is in Programmer Mode).

Instructions for using the PME and typical application examples are provided in the various manuals. See Chapter 9 for information on the set of safety logic instructions and function blocks available for safety applications.

Notes: Only these instructions & safety function blocks should be used for application logic development in the VersaMax SafetyNet System.

6.3 Hardware and Software Versions

The PACSystems VersaMax SafetyNet System components IC695CPS400 controller and IC200SBI001 Safety Network interface module have fixed firmware versions which can be used in safety applications. Do not upgrade the firmware versions for these components unless instructed by Emerson and then in accordance with the upgrade instructions provided in this manual. The hardware versions of all the components of PACSystems VersaMax SafetyNet System are also fixed. The specific versions of each component are listed in SIL certificate.

6.4 Application Software

The PACSystems VersaMax SafetyNet System identifies the application program in the runtime system with CRC values viewable in PME. There is a CRC value for application program on IC695CPS400 controller and hardware configuration. The CRC values are calculated by the controller at download time and can be used as part of your software modification procedures.

Section 7:Security

The PACSystems VersaMax SafetyNet System shall be protected against deliberate, illegal intrusion. In PACSystems VersaMax SafetyNet System “Enhanced Security” shall be used as a standard practice. It is the responsibility of the user of the safety system to establish and maintain adequate network security measures adapted to the level of openness in the particular installation for various cyber threats. Refer to the PACSystems™ RXi, RX3i and RSTi-EP controller Secure Deployment Guide (GFK-2830) for reference.

Section 8:Safety Function Blocks and Safety Instructions

PME will impose restrictions on the use of the safety function blocks for the IC695CPS400. The safety library created in PME for the IC695CPS400 will include a set of safety instructions and safety function blocks that can only be used by the application user for configuring safety logic. All the standard safety function blocks, standard LD blocks, and standard ST blocks included in the ToolChest or PME templates contain version information for tracking purposes. Refer to VersaMax SafetyNet Safety Function block document (GFK-3279) for details.

Section 9:Sample PME Templates and ToolChest for PACSystems™ VersaMax SafetyNet System

Sample PME templates and ToolChest are created for the PACSystems VersaMax SafetyNet System for user reference. The PME templates are created for CPS400 and VersaMax configuration respectively for 02, 04, 06, 08 and 10 remote I/O racks. It is highly recommended to use the sample templates as a starting reference for any project level configuration. The PME templates and ToolChest are both available on Emerson PACSystems/Movicon Customer Center for downloading. Both the templates and ToolChest have version information for tracking purposes.

In the PACSystems VersaMax SafetyNet System templates, while configuring, the user memory addresses are pre-defined, and users shall not modify them under any circumstances. These memory addresses shall not be used for any non-safety application. For non-safety applications, users can define addresses outside the safety addresses range.

Refer to the PACSystems™ VersaMax SafetyNet CPS400/SBI001 Templates IPI (GFK-3296) VersaMax Safety NIU Manual (GFK-3280) for further details.

⚠ WARNING

The latest PME Templates and ToolChest versions are always available on the Emerson Knowledge portal.

Section 10: Important Instructions for the PACSystems™ VersaMax SafetyNet System

- DNP3 protocol shall not be used in the PACSystems VersaMax SafetyNet system.
- PROFINET protocol shall not be used in PACSystems VersaMax SafetyNet system.
- Do not add printers and other non-essential devices on PACSystems VersaMax SafetyNet System network. It should be added on Plant business network.
- Use only Emerson approved unmanaged industrial ethernet switches in PACSystems VersaMax SafetyNet systems.
- Refer to Section 4.4 of FMEDA report for Application specific restrictions for VersaMax.
- RS485 serial port on IC200SBI001 shall not be used for serial communication with other devices.
- The Logic Checksum Words for IC695CPS400 shall be configured to 8192 words (as default setting) in PME.
- Do not add any user-defined logic in VersaMax SafetyNet Safety NIU IC200SBI001. It is strictly prohibited.
- IC200SBI001 Safety NIU does not support Expansion Modules, Communication modules and hence shall not be used in SafetyNet Systems.
- The default update timeout configuration for VersaMax IC200SBI001 is 500ms.
- The default Fail Wait Time for IC695CPS400 Safety controller is 300ms.
- The default Sweep mode for IC695CPS400 and IC200SBI001 shall be “Normal” only. User shall not configure it as Constant Window or Constant Sweep mode.
- Non-safety I/O modules and the logic associated with the non-safety I/O modules shall not be added/performed in the IC695CPS400 safety controller in PACSystems VersaMax SafetyNet system.
- The PACSystems VersaMax SafetyNet system shall be used with applications up to 2000 I/O points or less.

Contact Information and Support Guide

Questions? We are here to help.

Try searching the Knowledge Base system on our Customer Center website before starting a case or picking up the phone.

Search our Knowledge Base	Open a Support Ticket	Register for a Customer Account
pacsystems.co/knowledge	pacsystems.co/support	pacsystems.co/signup

Customer Center Home Page	Commercial Website	Contact Information
pacsystems.co/customercenter	pacsystems.co/commercial	pacsystems.co/contactus

Note: If the product is purchased through an Authorized Channel Partner, please contact the seller directly for any support.

Emerson reserves the right to modify or improve the designs or specifications of the products mentioned in this manual at any time without notice. Emerson does not assume responsibility for the selection, use or maintenance of any product. Responsibility for proper selection, use and maintenance of any Emerson product remains solely with the purchaser.