

PACSystems
Guide Form Specification

Version 1.1

February 19, 2021

Contents

Document Revision History 5
1 – General 6
Scope 6
Definitions 6
2 – Manufacturer's Standards 8
Industry Standards 8
Process Controller Standards and Agency Approvals 9
Design and Manufacture 10
Secure Development Life Cycle 10
Product Upgrades 10
Product Life Cycle 10
Documentation 11
Warranty 11
Preferred Vendor / Manufacturer 11
3 – System Architecture Overview 12
General 12
Overall Design 12
Simplex System Architecture Overview 13
High-Availability System Architecture Overview 14
Licensing 17
Controllers 17
FieldBus and I/O Support 17
Networking 18
Redundancy 19
System Reliability 21
System Architecture Drawings – Typical Systems 21
4 – System Configuration 26
Control Logic Developer 26
Multi-Discipline Controller Languages 26
On-Line Control Strategy 27
Instrument Index Definition and Management 27
Maintenance and Commissioning 27

5 – Fixed Backplane Controllers 29
General 29
Packaging 29
Environmental Conditions 29
Central Processing Unit 30
Multi-Discipline Controller Environment 31
Controller System Diagnostics 31
CPU Memory 32
Redundancy Synchronization and Failover 33
6 – Standalone Controllers for Simplex 34
General 34
Packaging 34
Environmental Conditions 34
Central Processing Unit 34
Multi-Discipline Controller Environment 34
Physical Requirements 34
7 – Rackless Controllers for High-Availability 35
General 35
Packaging 35
Environmental Conditions 35
Central Processing Unit 35
Multi-Discipline Controller Environment 36
Controller System Diagnostics 37
CPU Memory 38
Redundancy Synchronization and Failover 39
8 – Edge Controllers 40
IICS: Edge Controller 40
Physical Requirements 42
9 – I/O Systems 43
General 43
Packaging 44
Environmental Conditions 44
Discrete I/O 45

Analog I/O 48
Intrinsically Safe (IS) I/O 49
HART 51
Specialty Modules 52
I/O Time Stamping 53
10 – Industrial Switches 56
General 56
Industrial Ethernet Switch Types 56
Packaging 56
Environmental Conditions 56
Performance and Connectivity 57
Reliability 57
Monitoring 57
Redundant Ring 57
Security 57
PROFINET Capabilities 58
Additional Capabilities 58
11 – Security 59
Cyber Security 59
Advanced Cyber Security Features 59
Application Security 59
Additional Cyber Security Products and Services 60
12 – Industrial IoT 61
General 61

Document Revision History

Version	Revision Date	Description	Approved By
1.0	Apr 24, 2020	Initial creation of Emerson PACSystems Guide Form Specification	Product Management
1.1	Feb 19, 2021	Added support for OPC UA Non-Transparent Server Redundancy	Product Management

Document Updates

This document is only to be modified by Emerson's machine automation solutions business' product management team

1 – General

Scope

This specification covers the technical requirements for a control system to execute critical control over a process or a machine. This specification will cover hardware, software, and network requirements for control systems in simplex and high availability configurations.

Definitions

PLC: Programmable logic controller

PAC: Programmable automation controller

PNS: PROFINET Scanner

PNSR: PROFINET System Redundancy

MRP: Media Redundancy Protocol

Edge Controller: A controller that use real-time hypervisor technology to run real time deterministic control applications on real time operating system concurrently with the PACEdge software stack on a general-purpose operating system such as Linux in a safe a cooperative manner without one OS impacting the other.

Redundant IP: a floating IP Address which is used to provide redundancy in a hot standby configuration. It is used when IP addresses takeover where multiple machines are used for administrative access.

HMI: Human Machine Interface. The technology used to provide a graphic representation of data from a process and to accept user commands to be fed back to the process.

Ethernet: A high-performance local area network standard providing the two lower levels of the ISO/OSI seven-layer reference model, the physical layer and the data link layer.

TCP/IP: A protocol widely used across Ethernet networks for connecting computers and programmable controllers.

OPC UA: OPC Unified Architecture is a machine to machine communication protocol for industrial automation developed by the OPC Foundation.

Data Concentrator: A physical device that translates analog and digital information from attached I/O devices to a protocol that can be used with an HMI.

Communications Protocol: A formal set of conventions governing the control of inputs and outputs between the two communicating processes.

Network: An interconnected group of nodes, a series of devices, nodes or stations connected by communications channels.

Operating System: A program that controls the overall operation of the computer system hardware/ software.

Switch: A network device used to link computers, controllers and I/O devices.

PSIRT: Product Security Incident Response Team

2 – Manufacturer's Standards

The manufacturer shall have shown high commitment to product, manufacturing and design process quality. The manufacturer shall have attained ISO9001 certification and shall provide both hardware and software.

Industry Standards

The Redundant Control System shall conform to and take advantage of industry and de-facto standards. These shall include, but not be limited to:

- ODBC
- OLE
- ActiveX
- C programming language
- Visual Basic®
- Microsoft Windows
- Ethernet/IEEE 802.3
- TCP/IP
- OPC
- OPC UA
- OPC UA Non-Transparent Server Redundancy
- PROFINET
- HART
- Profibus
- DeviceNet
- CANopen
- Foundation Fieldbus
- S88
- 21 CFR Part 11
- Modbus
- IEC 61131
- IEC61850
- IEC 60870-5-104
- DNP3
- SNMP
- LLDP
- IO-Link

Process Controller Standards and Agency Approvals

The process controllers shall be designed, manufactured and tested in accordance with recognized industrial standards.

AGENCY APPROVALS		
Type	**Standard**	**Comments**
Quality Assurance in Design/Development, Production, Installation & Service	ISO9000	Certification by Underwriters Laboratories and British Standards Institute
Industrial Control Equipment (Safety)	UL61010-1	Certification by Underwriters Laboratories
Process Control Equipment (Safety)	CSA22.2, 142-M1987 or C-UL	Certification by Canadian Standards Association or Underwriters Laboratories
Hazardous Locations (Safety) Class I, Div II, A, B, C, D	UL1604	Certification by Underwriters Laboratory
European EMC Directive	CE Mark	Certification by Competent Body for EMC Directive
European RoHS Compliance	CE Mark	Compliance with European Directives for Restriction of Hazardous Substances
Marine	ABS, DNV GL, LR	Any of the listed marine agency approvals will be sufficient

ENVIRONMENTAL		
Type	**Standard**	**Conditions**
Vibration	IEC68-2-6, JISC0911	1G @ 40-150Hz, 0.012in peak to peak @ 10-40Hz
Shock	IEC68-2-27 JISC0912	15G, 11ms
Operating Temperature		0°C to 60°C inlet standard without fans
Storage Temperature		-40°C to +85°C
Humidity		5% to 95%, non-condensing
Enclosure Protection	IEC529	Steel cabinet per IP54: protection for dust & splashing
EMC EMISSIONS		
Type	Standard	Conditions
Radiated, Conducted	FCC CISPR11; EN55011	Part 15, section J, Class A
EMC IMMUNITY		
Type	Standard	Conditions
Electrostatic Discharge	IEC801-2	8KV Air Discharge. 4Kv Contact Discharge
Radiated RF	IEC801-3	10Vrms/m, 80Mhz to 1000Mhz, modulated
Fast Transient Burst	IEC801-4	2KV: power supplies, 1KV: I/O, communications
Surge Withstand	ANSI/IEEE C37.90a IEC255-4	2.5KV [cmn, diff mode]; power supplies, I/O [12V-240V]
Conducted RF	IEC801-6	10V, 150Khz to 80Mhz injected for communication cables > 30meters
ISOLATION		
Type	Standard	Conditions
Dielectric Withstand	UL61010-1, UL840, IEC664	1.5KV for modules rated from 30V to 250V
POWER SUPPLIES	IEC1000-4-11	During operation: Dips to 30% and 100%, Variation for AC ±10%, DC ±20%

The manufacturer shall have a fully operational quality assurance and quality control program in place and shall comply with ISO9001 standards for "Quality Systems - Model for Quality Assurance in Design/Development, Production, Installation and Servicing".

Complete product documentation describing installation, operation, programming and simple field maintenance shall be available in paper format and electronically.

Design and Manufacture

The vendor shall be a company who regularly designs, manufactures and services process control systems, including the hardware controllers and the system software. The vendor shall be in the controls business for at least 30 years and shall have manufacturing operations in the United States of America with worldwide support capability.

The manufacturer shall have a fully operational quality assurance and quality control program in place. Complete documentation describing the quality assurance and quality plan shall be available.

The programmable automation controller and all the corresponding components within the family of controller products shall be offered by a company who regularly manufactures and services this type of equipment. It shall have attained ISO9001 registration.

Secure Development Life Cycle

The vendor must have an established development life cycle that allows for traceability of features and functions throughout that life cycle.

The vendor must have a formal and documented set of quality assurance procedures that are applied to the engineering design, development and documentation of the software. The presence of a formal quality assurance department shall be required.

The vendor must also demonstrate that its source code for the product is regularly archived both on-site and off-site in facilities suitable to withstand physical harm.

The vendor shall allow for on-site auditing of the development life cycle to ensure good practice.

The vendor should ensure cyber-security related testing with every release (firmware or software), and the vendor shall utilize Red Team vs Blue Team testing to verify the effectiveness of security measures

The vendor shall have a PSIRT group and a process in place to promptly handle computer security incidents.

The vendor shall also provide key documentation including secure deployment guides.

Product Upgrades

The manufacturer shall make product upgrades available for purchase. These upgrades shall include both functional upgrades to add features or product options and version upgrades to take the product up to the currently offered product version or revision level.

Product Life Cycle

The manufacturer shall have a published product life cycle policy.

Products shall be designed for a long operational life, typically ten years or more, with spares supply and support during the life cycle of the product. Modernization to later generation product shall be supported with the aim of minimum downtime and disruption to processes during modernization.

Documentation

Documentation on use, maintenance, configuration, controller hardware, software and I/O devices shall reside on the system as displayable text and graphics and be provided in paper format and electronically (via download or on disk).

The online help system in the product needs to be context sensitive such that immediate help is available for the selected functionality.

Warranty

Hardware Warranty

The manufacturer shall provide a warranty period of at least 2 year from the date of purchase for the hardware components of the system.

Extended warranty shall be available as a separately purchasable item.

Software Warranty

Vendor shall provide a 90-day warranty on all software provided with the system along with the option to purchase a software support contract. This contract is to include:

- Telephone and email support Mon-Fri 8:00AM to 8:00PM EST
- 24x7 emergency support
- Software upgrades
- 24x7 access to web-based technical and support information

The vendor shall have a location on their website where users can download software improvements, bug fixes, add-ons and components.

The vendor shall provide an easy mechanism for upgrading and installing software improvements and for allowing a user to quickly ascertain what improvements have been installed.

The manufacturer or its authorized representative shall provide complete technical support for all the products. This shall include headquarters or local training, regional application centers, local or headquarters technical assistance and a toll-free hotline shall be available for technical support.

Post Warranty Support

Post-warranty support shall be available as a separately purchasable item.

Preferred Vendor / Manufacturer

Pre-evaluation has identified the Industrial Automations and Control Systems products from Emerson's controls as the preferred solution. Any proposed solution must include, at a minimum, the functionality contained in the current commercially available version of these products.

3 – System Architecture Overview

General

This section of the specification covers requirements for the supply and fabrication of an industrial automation control system application. The intent of this section is to provide a guideline for specifying hardware, software and configuration architecture for small to mid-sized industrial automation control system, to monitor and control a manufacturing process or a facility.

Overall Design

The system shall consist of rugged components designed specifically for industrial environments. A complete system shall consist of one or more racks containing controller, communications modules and I/O modules, interconnected by signal cables.

The hardware of the system shall be designed to operate with a variety of remote I/O drops including RX3i PROFINET I/O Scanner (PNS), RX3i CEP, VersaMax PNS, RSTi-EP PNS and PAC8000 Process I/O PNS. It shall support industry standards, be modular in design and adopt industry standards to allow easy integration with other manufacturing systems.

The system shall provide a comprehensive set of software for the following:

- programming the automation controllers
- configuring the hardware
- monitoring the operation of the controller
- diagnosing faults

For both simplex and high availability applications, the system shall provide the following:

- **Software capable of:**
    - Programming the process controllers
    - Configuring the hardware
    - Monitoring the operation of the controller
    - Diagnosing faults
    - Automatically enforcing incoming and outgoing traffic type based on user configuration through a built-in firewall that can and can manage packet for communications ingress/egress throttling
    - Locking and encrypting user logic with a password
    - Verifying secure digitally signed firmware updates
    - Allowing directive access to user memory based on password privilege level, even in the programming tool
- **Hardware including:**
    - Embedded switches on slave modules

- Passive cooling, without the use of any fans
- Support for exchanging device health and connectivity information automatically through cyclic IO
- Controllers with TPM module which support secure boot
- Backplane communication speed of at least 1gb/sec
- Controller with at least one embedded GB ethernet port
- Ability to natively monitor and synchronize two power grids (ranging in voltage from 120 – 600 vac)
- Support for more than 200 hart IO points per remote IO drop
- Support for remote IO drops as far as 10km without external ethernet switches
- Support for immediate conversion on remote IO drop: copper to both types of fiber and can switch between fiber multi-mode, fiber to multi-mode copper to single mode, or multi-mode to single mode
- Support 1.5 MHz high speed counter
- System should be capable of supporting sequence of events (SOE) with 1ms accuracy across all IO points for at least 512 configurable SOE points

The system architecture shall be arranged for simplex and high availability applications to best fit the application's need and the software shall allow the customers to migrate their application code between simplex and high availability architectures seamlessly.

The system architecture for simplex and high availability applications is described in the section below.

Simplex System Architecture Overview

In a simplex application, the system architecture shall include the following:

- High performance controllers with minimum 1MB of retentive memory including capability for storage and upload of documentation
- Standalone controllers with minimum Achilles Level 1 certified, such as: RSTi-EP CPUs, RX3i CPL410, RX3i CPE400
- PROFINET architecture that supports the Media Redundancy Protocol (MRP) with features such as named remote IO drop
- IO network communication speeds should be a minimum of 100Mbps
- Chassis based backplane controllers shall support minimum 1x1Gb Ethernet interface
- Standalone controllers shall support minimum 3x10/100 Ethernet interfaces
- Controllers may support secure encrypted communication between controllers and HMI

High-Availability System Architecture Overview

The system shall support at least basic and advanced high availability architectures meeting the following requirements:

- **Basic High Availability Architecture** - System shall support hot-standby controllers synchronized by dedicated high speed synchronization links of at least 1Gbps and a minimum switchover time of 300ms and shall include the following
    - IO network communication speeds should be a minimum of 100Mbps
    - Controller with at least 4x1Gbps embedded Ethernet ports
    - Support for full data synchronization between active and backup controllers by scan, rather than synchronization by exception
    - Minimum 1Gbps dedicated connection between active and standby controllers
    - Support for at least 20 remote IO drops in a ring without external ethernet switches
    - Fault-tolerant I/O network using ring topology
    - Support for 10ms MRP ring recovery
    - Minimum 64MB of retentive memory including capability for storage and upload of documentation
    - Redundant IP support capabilities
    - Ability to support different firmware versions between active and backup in synchronized systems
    - Support for named remote IO drop
    - Support for secure encrypted communication between controllers and HMI
    - Controllers which are Achilles Level 2 certified such as the RX3i CPE400 and RX3i CPL410.

- **Advanced High Availability Architecture** - System shall support hot-standby controllers synchronized by dedicated high speed synchronization links of at least 2Gbps and shall have “bumpless” switchover with a switchover time of one controller scan (typically 5-20ms). Furthermore, it shall include the following
    - IO network communication speeds should be a minimum of 100Mb/second
    - Support for up to 10km of distance between primary and secondary controllers
    - Support for at least 60 IO drops in a ring without external ethernet switches
    - A minimum 2.12Gbaud dedicated connection between active and standby controllers

- Option to support hot-swappable PROFINET Controller
- Support for local IO in the rack
- Support of at least 64 remote IO drops without external ethernet switches
- Fault-tolerant I/O network using ring topology
- Support for redundant communications to higher level systems such as HMI/SCADA
- High performance controller with at least 2x1Gbps embedded ethernet ports
- Redundant IP support capabilities
- Support for 10ms MRP ring recovery
- Minimum 64MB of retentive memory including capability for storage and upload of documentation
- Ability to support different firmware versions between active and backup in synchronized systems
- Support for full data synchronization between active and backup controllers by scan, rather than synchronization by exception
- Support for named remote IO drop
- Support for secure encrypted communication between controllers and HMI
- Controllers which are Achilles Level 2 certified such as the RX3i CPE330

See figures 3.1, 3.2, and 3.3 for representative system architectures.

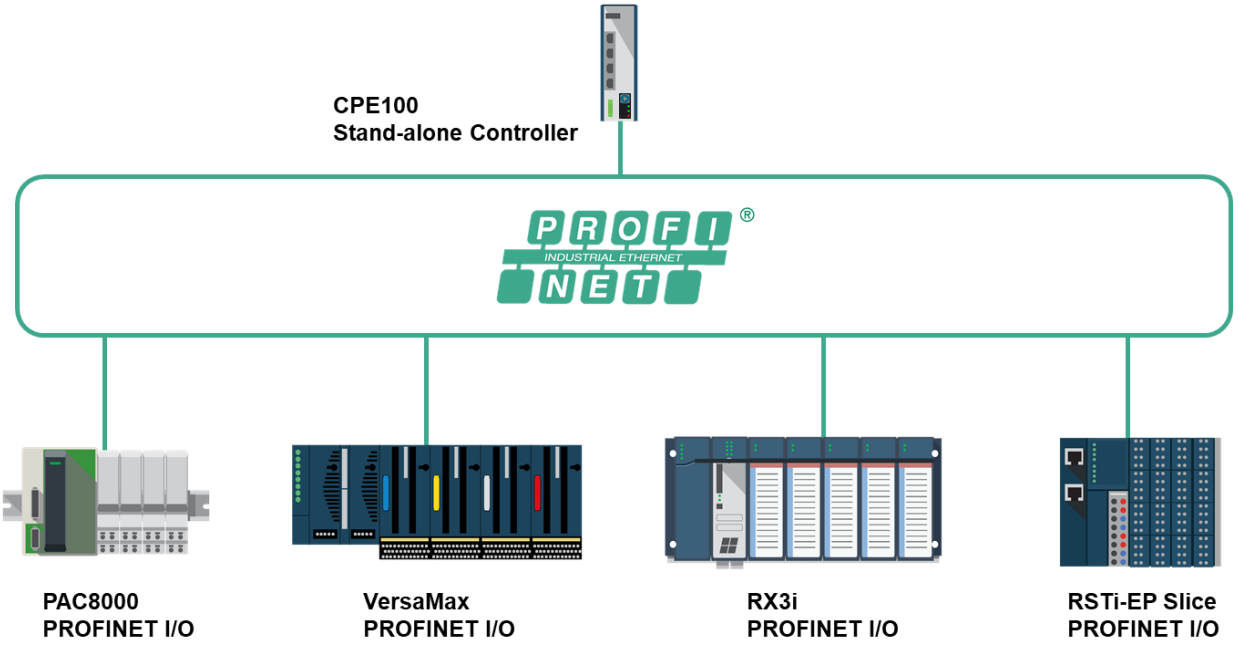


Figure 3.1 Simplex System Architecture

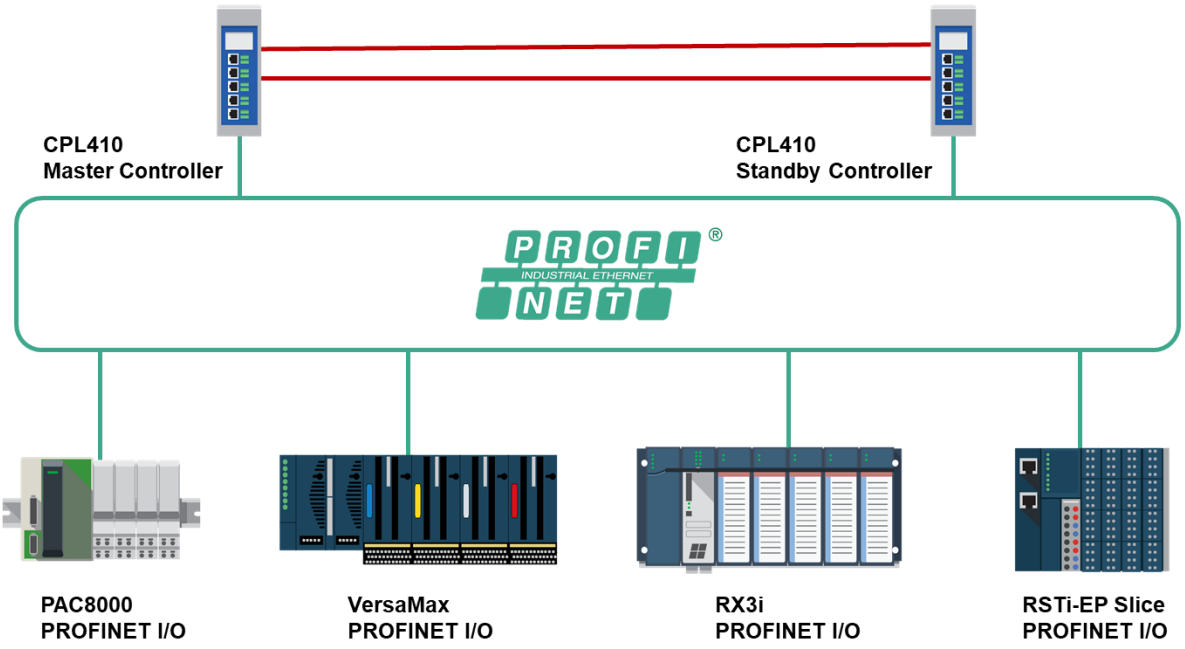


Figure 3.2 Basic High Availability System Architecture

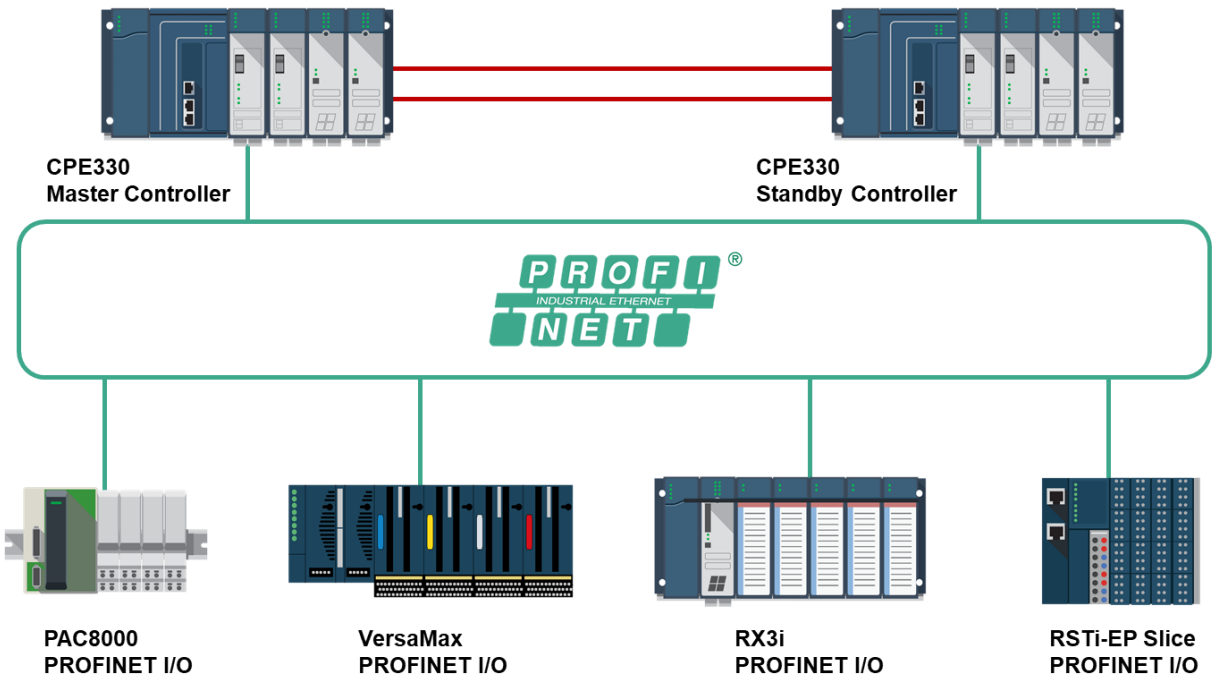


Figure 3.3 Advanced High Availability System Architecture

Licensing

Licensing for redundancy shall be built into the controllers with no additional purchase of licenses required.

Licensing for configuration and programming software shall be by cloud-based license server with support for local software or hardware-based authorization. Licensing for Virtual Machine shall be supported. Configuration and programming software shall be licensed directly by the Vendor or its Affiliates

Controllers

The automation controllers are responsible for running and executing the control strategy in real time with the devices and plant equipment. Backplane controllers shall be available with a backplane communication speed of at least 1 Gbps.

The controllers must be capable of supporting the full spectrum of control applications including discrete, continuous and batch.

FieldBus and I/O Support

Fieldbus Support

The system shall support at a minimum the following fieldbuses through either direct connect or proxy

to the LAN:

- PROFINET
- HART
- Foundation Fieldbus
- Profibus DP/PA
- GE EGD
- DeviceNet
- CANopen
- Modbus TCP
- IEC61850
- IEC 60870-5-104 (IEC104)
- DNP3

I/O Support

The system shall support at a minimum the following I/O devices for high availability applications:

- VersaMax I/O
- RX3i I/O (PNS and CEP)
- RSTi-EP I/O
- PAC8000 Process I/O

In addition, the system shall support at a minimum the following I/O devices for simplex applications:

- VersaMax IP I/O
- RSTi I/O
- VersaPoint I/O
- VersaSafe safety system

Networking

The system shall support Ethernet as the network for communications between the engineering workstations and the controllers. The following network architectures shall be supported:

- Simplex – A single network path runs from the computers to the controllers.
- Media Redundancy – A redundant protocol that provides each node on the network with a backup physical connection to every other node on the network in a ring topology. It shall support I/O update rates as fast 1ms. It shall run over networks up to 1Gbps inspeed. It shall support network recovery as fast 3ms, without requiring packet duplication on the network.

Redundancy

The principle of redundancy in automated systems provides for switchover of functionality to a backup component in case of failure of a primary component. The switchover is considered automatic if no operator intervention is required. Redundancy applies to both hardware and software and implies minimal loss of continuity during the transfer of control between primary (active) and redundant (backup) components.

Redundant systems reduce single points of failure, preventing loss of functionality. The major levels of redundancy shall include:

- Automation Controller
- Media redundancy
- I/O network
- HMI SCADA network

Each level of redundancy provides a failover system that allows continuous system activity with minimal loss of data. The following sections briefly describe each level.

Automation Controller Redundancy

The system shall support process controller redundancy. Controller redundancy lets control transfer from a primary controller to a hot stand-by redundant one in case of failure. When the primary controller comes back online, control can be transferred from the redundant controller back to the primary with minimal loss of data. The redundancy can be synchronous. Synchronous systems coordinate control and handling of data between CPUs of the active and backup units, while in independent systems each controller acts like an active unit and is not constrained by the others. Systems shall be updated while keeping the process running. System shall be checked out for commissioning or maintenance with only one controller in the system. System shall support for full data synchronization between active and backup controllers by scan, rather than synchronization by exception.

For high-performance applications, controller redundancy shall be provided via reflective memory through a high-speed (2.12Gbaud) fiber optic path between the controllers. Distance between controllers shall be up to 10 kilometers with no need of external devices between systems. Failover shall be “bumpless” with a failover time of one controller scan (typically 5-20ms).

For less demanding applications, controller redundancy shall be provided via 1Gbps Ethernet through a high-speed dual cable path between the controllers. Distance between controllers shall be 100 meters with no need of external devices between systems or up to 10 kilometers using external devices. a Failover time should be at least as fast as 300ms.

Media Redundancy

The system shall support PROFINET over Media Redundancy Protocol (MRP), a redundant protocol that provides each node on the network with a backup physical connection to every other node on the network in a ring topology. It shall provide deterministic real time I/O control with support of updates of 1ms and shall transmit at a minimum 100Mbps speed.

The network shall not limit bandwidth by transmitting in two directions. The network shall transmit in one direction and when it senses a cut off in transmission, reroute the data in order to not lose control of the I/O.

The system shall work seamlessly with other products that implement the MRP standard.

The system shall provide diagnostics to identify failure of a cable, network port and network nodes. These indications shall be available automatically in the customer's process data.

The system shall include the ability to set up both ring, and sub-ring network structures. In a ring-shaped network, switches will allow for recovery times of less than 30ms in case of a failure. Sub-rings shall be available to integrate new network segments existing ring networks.

I/O Network

The system shall have the ability to configure and monitor all ethernet devices used in the network. The system shall have the ability to configure and monitor all ethernet devices in the redundant configuration.

LAN Controller and LAN Scanner

The LAN controller shall support PROFINET and it will be integrated into the overall system configuration. It supports at least 100Mbps Ethernet speeds.

The LAN controller controls up to 64 devices and has the ability to update I/O in 1ms.

The LAN controller will have two built in RJ-45 ports and support two additional SFPs (small form factor pluggables) for providing additional connections. The SFPs shall allow a customer to use copper, multimode, or single-mode fiber without having to use a media conversion device.

The LAN controller shall have a built-in switch, so the network connections do not need to have external switches in the ring.

The LAN controller shall be able to pass through other protocols with minimal effect on I/O LAN in order to have other devices such as operator interfaces supported at the remote drop without additional switches, wiring, or local control.

The LAN scanner shall have capability to support copper or fiber direct connect with a built-in switch. No external or third-party switches shall be required. The vendor shall supply a range of PROFINET-enabled switches if a switch is required, for example for connection of third-party equipment.

The LAN scanner for rack-based I/O shall have the same hardware as the LAN controller to support different media and switch-through protocol. It shall have support for a media card to load in configuration directly if it needs to be replaced while in operation.

The LAN controller and scanner shall support Simple Network Management Protocol (SNMP) and Link-Layer Discovery Protocol (LLDP) data, which can be used by standard IT-style tools to monitor the network.

Cabling Redundancy

The system shall support separate physical connections to the same device using redundant network

cables and connections. The devices can be on a LAN or may require serial connections. Redundant cabling provides an alternate communication path to the device if the association with the host computer is lost due to failure of the primary path. The implementation of cable redundancy with respect to host monitoring/control systems differs with the device protocol involved.

Computer (Operator Station) Redundancy

The system shall support computer redundancy. Computer redundancy of the system shall provide protection such that the failure of one operator station does not affect the performance, monitoring, or control capabilities of other operator stations.

Computer Network Redundancy

The system shall support Computer Network Redundancy. Computer network redundancy is similar to cabling redundancy, except it covers computer-to-computer communications rather than computer-to-process-controller. Computer network redundancy provides an alternate network path in case of failure of the primary network.

OPC UA Non-Transparent Server Redundancy

All systems that support PNSR shall also support OPC UA Non-Transparent Server Redundancy. This provides data structures to allow the client (HMI SCADA) to identify which servers are available in the OPC UA Redundant Server Set and what modes of failover the server supports. This information allows the client to determine what actions it can take on failover to continue receiving OPC UA communications from a redundant server set.

System Reliability

The system shall include fault tolerance to assure that no processor component or communication failure anywhere in the system will cause the operator to lose control of status of the process. The system shall be provided with redundant processors, servers, power supplies and distribution for all control and communications functions.

System Architecture Drawings – Typical Systems

Water and Wastewater Plant

Figure 3.4 shows a control system for a small to mid-sized water or wastewater plant comprising of a high availability system including high availability HMI/SCADA. Figure 3.5 shows an architecture for mid to large sized.

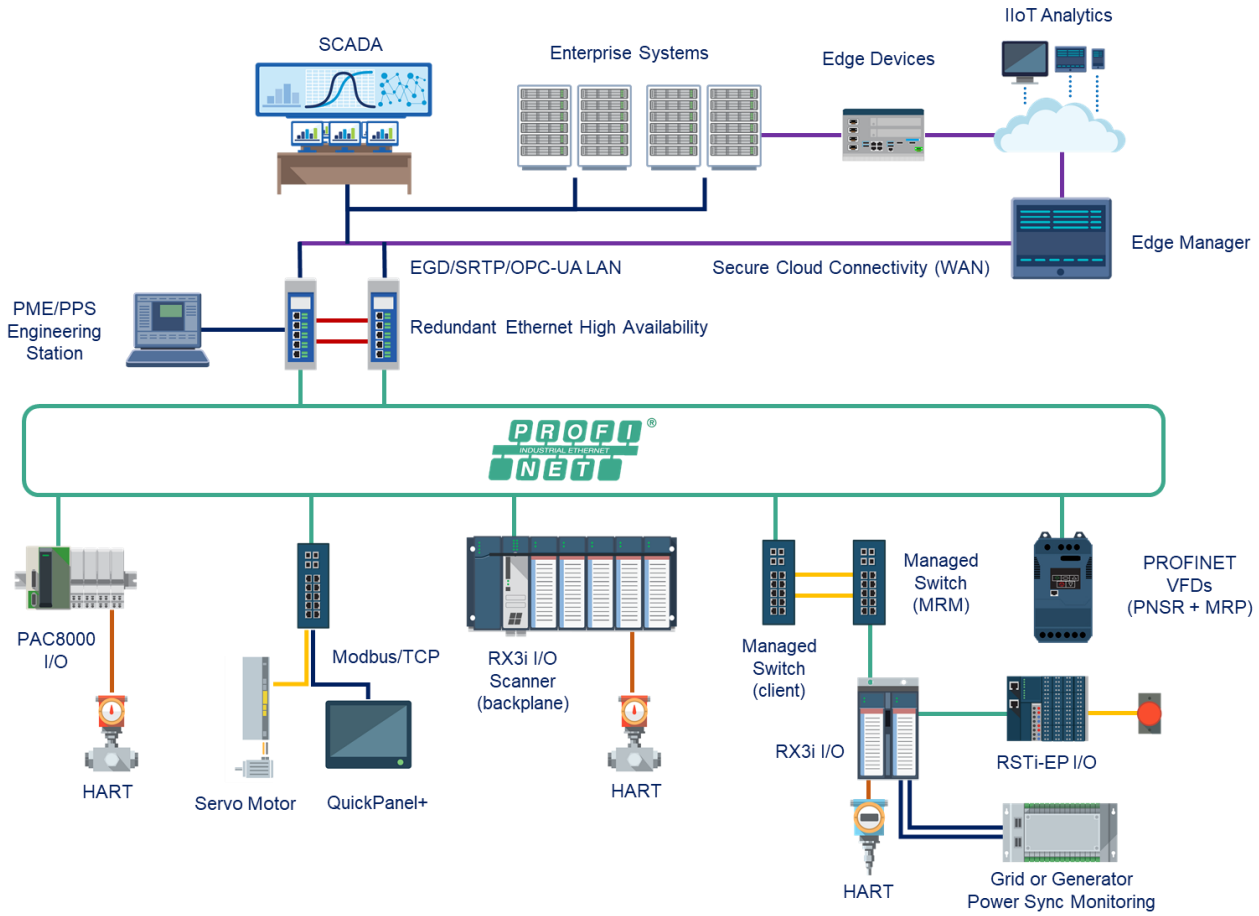


Figure 3.4 System Architecture – Water and Wastewater Small to Mid-Size

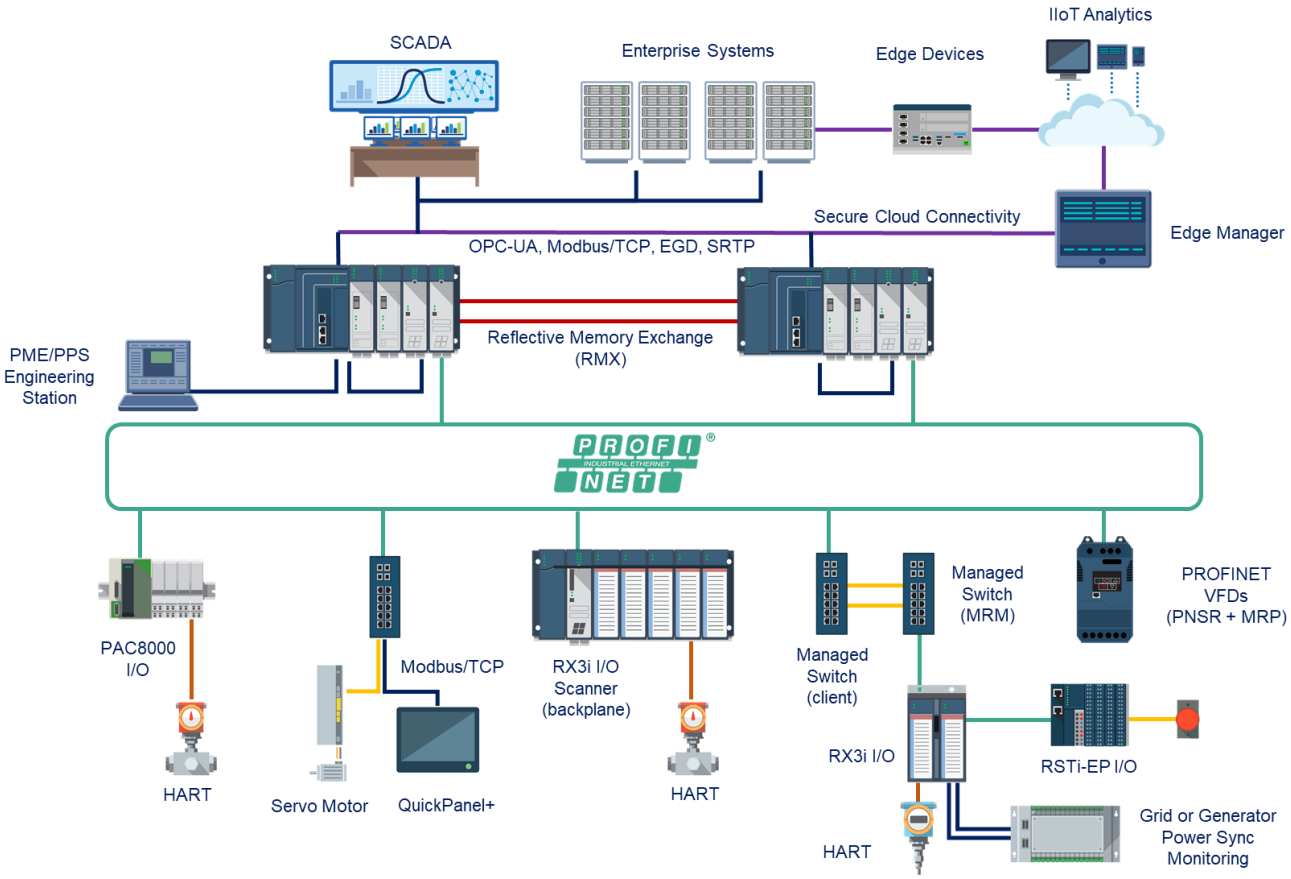


Figure 3.5 System Architecture – Water and Wastewater Mid to Large Size

Hydro Control System

Figure 3.6 shows a control system for a small hydro plant comprising of a high availability system including high availability HMI/SCADA. Figure 3.7 shows an architecture for mid to large sized.

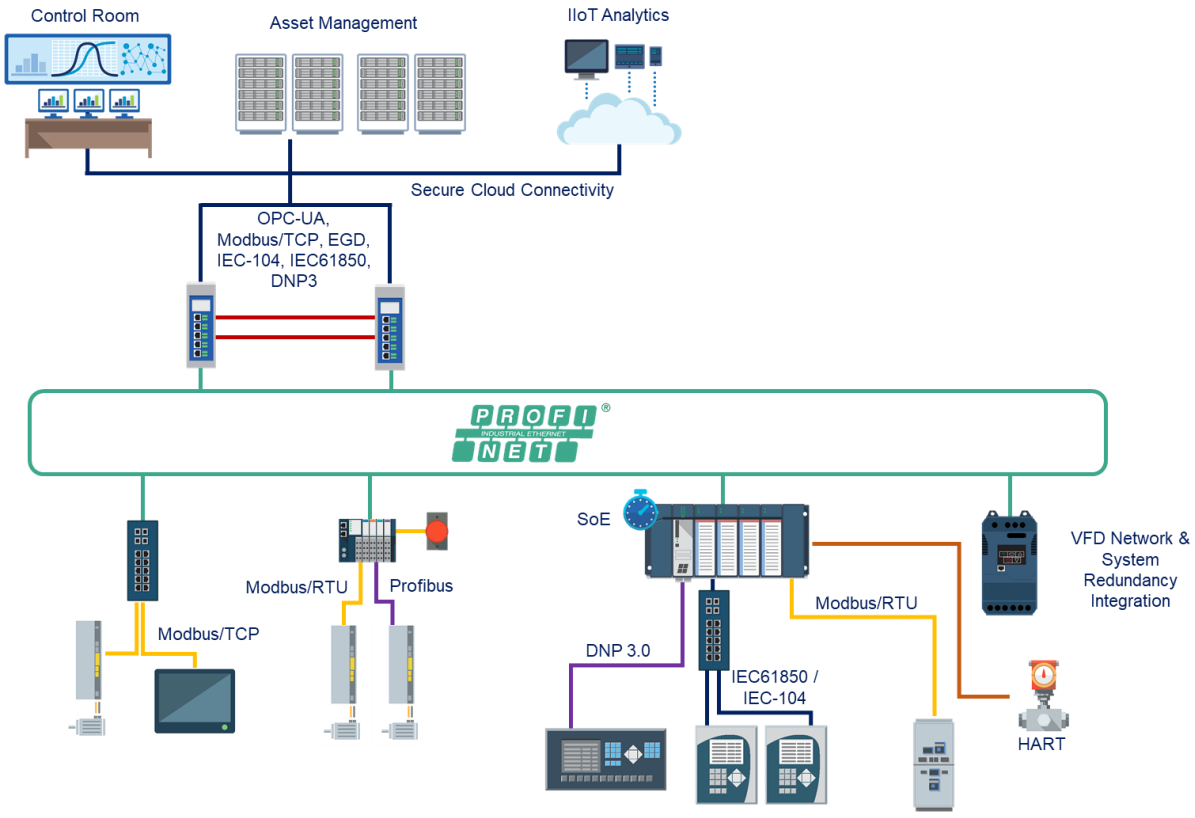


Figure 3.6 System Architecture – Hydro Small

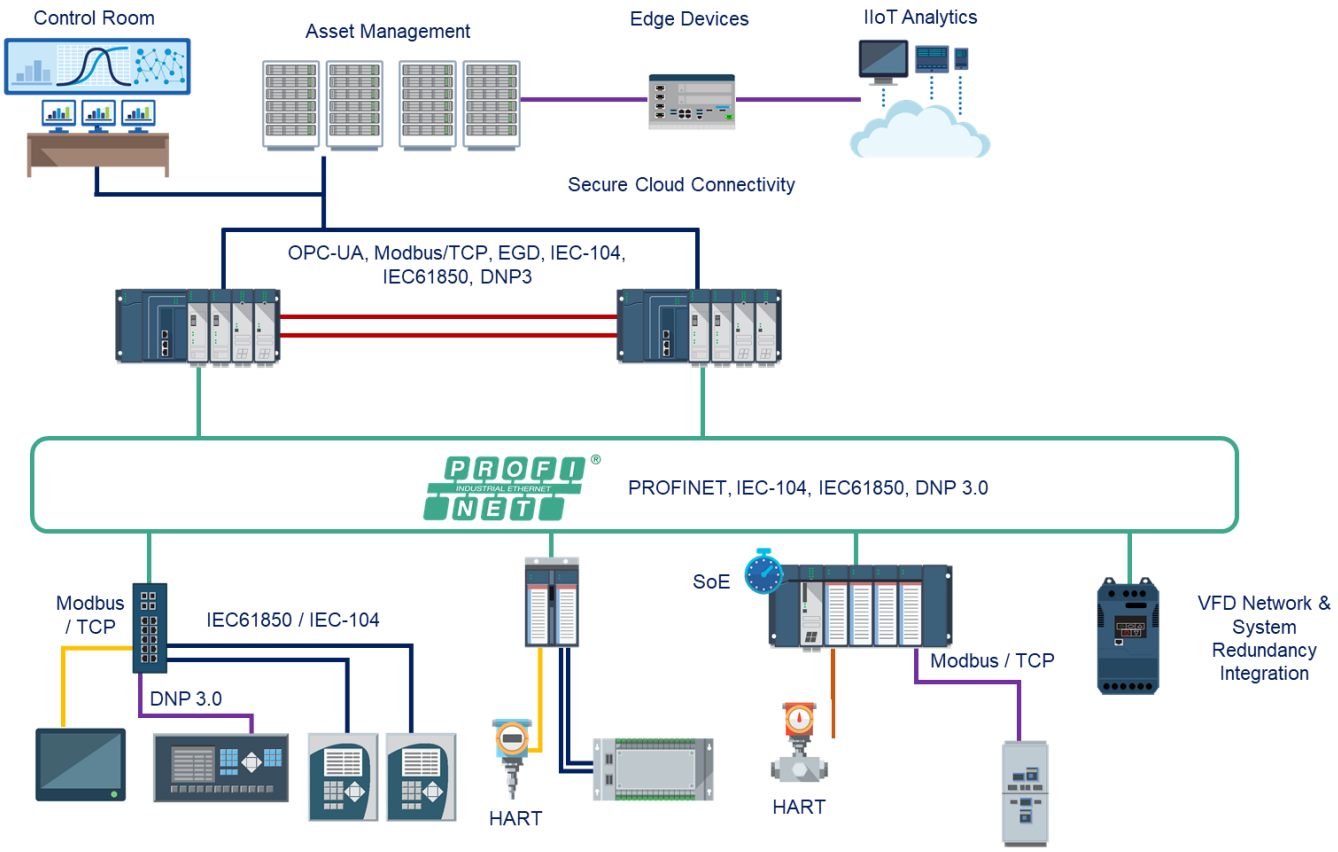


Figure 3.7 System Architecture – Hydro Mid to Large

4 – System Configuration

The engineering workstation shall host the control logic developer and visualization configuration. The control logic developer shall support the ability to create and edit the control programs that will run in the process controllers. The logic developer shall allow the user to view a navigation pane, drawing pane and properties pane in the same window at the same time. Selecting different function blocks within the drawing pane shall show their properties in the property pane.

Control Logic Developer

The control logic developer shall run on an engineering workstation, such as PAC Machine Edition Integrated Development Environment. The control logic developer shall will be IEC 61131-3 compliant in at least the following languages: Structured Text, Function Block Diagrams, and Relay Ladder Logic.

When in programming mode, the controller is connected to the logic developer software for downloading and monitoring the developed program. Version control, tracking and auditing of logic programs and visualization screens shall be provided by PAC Change Management. Through a checkout and check-in procedure, PAC Change Management will allow multiple engineering workstations and collaborative devolvement while preventing multiple people from changing the same aspect of the system at the same time.

Programming Languages Supported

The control environment shall support the ability to program in Function Block Diagrams, Structured Text, Ladder Logic and C.

Redundancy Configuration

The Engineering workstation shall be used to configure the parameters of a redundancy system, including the following:

- Configuration of primary and secondary hardware configurations, including PROFINET controllers and PROFINET I/O.
- Redundancy Wizard to select and configure redundancy modules.
- Function to mirror primary hardware configuration to secondary hardware configuration.
- Configuration of redundancy transfer lists.
- Configuration of redundant IP address.

Reusable Control Logic

The control logic developer shall provide the ability to create user defined function blocks and types which can be instantiated multiple times in the program.

Multi-Discipline Controller Languages

Controllers in the system must be multi-discipline (allowing for Function Block, Ladder, Structured Text and C) to be handled at the same time. There shall be a single logic developer capable of programming the controllers in the multiple languages.

On-Line Control Strategy

It shall be possible to modify control strategies on-line without disrupting the operation of other executing control loops. The system shall be capable of modifying a single program file, single control strategy drawing, or single block without affecting the operation of other control loops in the system. The system will track the control strategies downloaded to the controller and clearly provide information to the users on which control strategies have been downloaded to the controller. It shall be possible to put associated control loops in manual mode prior to performing the online change. Outputs shall be held at their last value during an on-line program change.

It shall be possible to drag and drop function blocks from a library into the drawing environment. It shall also be possible to drag and draw connections between the outputs of blocks and the inputs of subsequent blocks.

The system shall show the user any forced variables by underlining the values and allowing for a different color animation. When the controller is off-line, the programming environment shall show the configured initial values. When the controller is on-line, the programming environment shall show the current values as they exist and are updated in the controller. When the program is executing, the environment shall show the animation of the logic “wires” in the drawings.

The environment shall provide tooltips to display details on variables.

The CPU or coprocessor shall be capable of being protected by a security password to prevent unauthorized people from making modifications to the program.

The system configuration may be changed in a redundant operation while running.

The LAN remote I/O drops shall be able to be configured through the system. The remote I/O drops shall be addressed by IP address and name-based configuration based on PROFINET open standard protocol.

Each I/O device in the LAN shall have a GSDML configuration file based on PROFINET standard protocol so to be used by any standard PROFINET controller.

Instrument Index Definition and Management

The vendor shall offer software with instrument index information stored in a database. The information collected with each I/O point shall include test status, factory acceptance testing results, and site acceptance testing results. Information for PROFINET I/O including, device name, network information, device type, and vendor shall be provided.

Maintenance and Commissioning

The system shall provide the ability to animate the control strategies with current values of the I/O and intermediate values read from the controller. The viewer shall provide the ability to turn animation data on and off, access and set the tuning parameters for blocks that can be tuned and display the scaled and raw values for each I/O and intermediate value. The system shall maintain a cross reference of variables used in the control strategies with the physical diagrams where they are used. The system

shall provide a capability to quickly locate a common variable used on another control strategy diagram.

The vendor shall offer software with capable of displaying HMI graphics and the animated control strategies in the viewer simultaneously, with the objective of seeing the impact of HMI changes on the running control strategies.

5 – Fixed Backplane Controllers

General

The system shall consist of rugged components designed specifically for industrial environments. A complete system shall consist of one or more racks containing I/O modules, interconnected by signal cables. The PACSystems RX3i CPE330 is an example of such a controller.

Packaging

All components shall be housed in structurally secure enclosures.

The controller CPU shall be modular. It shall be fully enclosed within a durable plastic or metal shroud. When mounted on the system base, the modular CPU shall not occupy more than two available slots. The controller CPU shall be passively cooled

There shall be at least three sizes of base available, supporting 7, 12 and 16 modules. The base shall support a high-speed serial bus and a high-speed PCI bus.

Removing the module shall require no special tools.

Modules shall connect electrically to the baseplate via a pin and socket connector.

Modules shall be fully enclosed in a plastic or metal covering protecting the electronic circuitry from exposure (IP20 protection).

Base shall include an integrated grounding bar at the bottom of the base for securing shields and commons from field devices to minimize noise into the modules.

Wherever possible, all assemblies and sub-assemblies performing similar functions shall be interchangeable.

The system design shall accommodate the replacement of assemblies without having to disconnect field wiring. Wherever possible, removable connectors shall be used to connect field wiring to the individual circuit board assemblies.

All major assemblies and sub-assemblies, circuit boards and devices shall be identified using permanent labels or markings, each of which indicates the manufacturer's catalog number, product manufacturing date code, UL and C-UL and CE certifications.

Environmental Conditions

PCI backplane controllers shall meet the following environmental specifications.

Operating Environment:

Hazardous Area Location:	ATEX Eex nA IIC T4
Field wiring:	ATEX 3G Iic T4 –nL
Temperature:	0 to 60 deg C (32 to 140 deg F)
Airborne Contaminants:	IAS-S71.04 – 1985 Airborne Contaminants Class G2

Storage Conditions:

Temperature:	-40 to 85 degrees Celsius

Operating Conditions:

Temperature:	0 to 60 degrees Celsius
Humidity:	5 to 95% relative humidity, non-condensing

A low temperature testing service shall support operation from -40 to 60 degrees Celsius.

Central Processing Unit

The CPU offered shall be a modular type. The CPU shall possess the capability to solve application logic, store the application program (including documentation of variable names, rung comments and documentation files), store numerical values related to the application processes and logic and interface to the I/O systems. The CPU shall need no additional modules to provide at least the following advanced programming features: floating point math, PID, modulo, math, double precision math, logical functions, subroutines, data array move and indirect addressing.

Modular CPU

The vendor shall offer a modular type CPU shall containing the following: A minimum Intel or compatible dual-core microprocessor operating at speeds no less than 1GHz as the main processing element, memory mounted on the board. A minimum of 2Mb of user memory shall be on board for user configurable application, data storage and documentation storage. User memory will be backed up by built-in Flash memory of the same capacity as the user memory.

The modular type CPU shall contain a real-time calendar and clock that can be accessed by the user program. This Time of Day clock and calendar shall be battery-backed and maintain seven time functions: year (2 digits), month, day of month, hour, minute, second and day of week.

The modular CPU shall execute Boolean functions at a rate of 0.3 microseconds per instruction or lower.

The CPU shall provide either serial ports or Ethernet ports for communications. On all available CPUs, ethernet shall be at least $10/100Mbs^{-1}$ with at least one port for connection. An available CPU model shall include ethernet of $10/100/1000Gbs^{-1}$ with at least two ports for separate connections. On this advanced CPU, one port shall support PROFINET Controller functionality with a built-in switch and MRP protocol for PROFINET network redundancy.

A RUN ENABLED/RUN DISABLED/STOP switch shall be on the CPU behind a door for security.

LEDs on the CPU shall indicate the following:

- CPU OK
- RUN mode
- Outputs Enabled
- I/O Force

- Battery condition
- System faults
- Communications activity

Multi-Discipline Controller Environment

The controller shall be capable of supporting process, discrete and batch applications at the same time.

Cyber security

The controller CPU shall support the following:

- Secure boot
- TPM (Trusted Platform Module)
- Secure firmware updates
- Multiple password-protected levels of access with increasing privileges
- Secure and encrypted communications
- Encrypted passwords
- Disabled unused network ports
- Throttling on Ingress/Egress communications on Ethernet ports
- Redundant controller shall be Achilles Level 2 certified

Controller System Diagnostics

Visual Diagnostics

LEDs on the CPU shall provide a status display for the CPU.

Alarm Processor

The CPU shall contain an alarm processor that is special process controller feature designed to receive and process faults. The diagnostics shall provide information on the configuration and CPU, memory, communications and I/O status.

The alarm processor function shall log I/O and system faults in two fault tables that shall be accessible for display on the PC compatible programming software screen or uploaded to a host computer or other coprocessor.

The alarm processor shall maintain the states of up to 128 discrete system diagnostic bits to be read by a host or incorporated as contacts into the ladder program for customized diagnostic routines.

Each fault table shall have a total capacity of 32 faults. The last 16 entries shall maintain the latest 16 faults. The first 16 shall be kept unchanged.

Faults may be cleared by the user by way of a programmer. Provision shall be made by way of passwords to protect these faults from unauthorized clearing.

Alarm Features

The alarm processor shall report three types of fault action; fatal, diagnostic, or informational and the CPU shall respond as follows:

Faulty Action	Fatal	Diagnostic	Informative
CPU Enters STOP Mode	Yes	No	No
Set Diagnostic Bit	Yes	Yes	No
Logged In Fault Table	Yes	Yes	Yes

When an I/O fault occurs, the alarm processor shall report the drop, rack and slot location of the fault, the condition, the address and the circuit number if appropriate.

This alarm processor function shall have the capability to time-stamp system faults for future references.

Version Information

The system shall have the ability to display serial number and date code in PME Device Information Details.

CPU Memory

Memory Capacity

The process controller shall supply a modular design CPU that contains at least the following:

- 2 - 64 MB for application programming. The redundant controller CPU shall have the 64MB of retentive memory including capability for storage and upload of documentation
- Configurable up to 4MB 16-bit registers for register and data usage
- Up to 32K control relays internal battery backed
- Up to 32K bits for discrete inputs
- Up to 32K bits for discrete outputs
- Configurable up to 32K 16-bit registers for analog inputs
- Configurable up to 32K 16-bit registers for analog outputs

All application memory shall be available to the user program. Executive level operations performed by the CPU shall not consume application memory.

Memory Storage

The application program and system configuration shall be stored in FLASH memory if so selected.

There shall be an energy pack of capacitors used to maintain the contents of the RAM memory in the CPU. The energy pack shall be replaceable with power applied to the process controller and without

removing the CPU. Batteries, except for small coin-cell types, shall not be used to avoid explosion and fire risk and to eliminate issues with shipping of equipment.

There shall be an easy connection for the energy pack to connect and be replaced while running.

An LED shall provide visual indication of the energy pack condition. Additionally, poor energy pack condition shall be alarmed with a system diagnostic bit.

The CPU shall allow resident user program to be maintained in the CPU without power applied. A CPU shall be able to be shipped without energy pack connected and the user program and data registers preserved in Flash memory.

The CPU shall calculate the application program checksum at the end of every sweep. A complete checksum calculation for a program may take several sweeps. A fixed number of program memory checksum shall be calculated each sweep. This number is configurable by the user. If the calculated checksum does not equal the reference checksum, a fault shall be recorded and the CPU mode will change to STOP.

The memory on the CPU shall be capable of storing support documentation such as Word, Excel, CAD and other files in both RAM and FLASH.

Redundancy Synchronization and Failover

The modular controller shall support high speed redundancy synchronization and failover using fiber-optic Reflective Memory (RMX) technology. The controllers shall be synchronized every scan. In the event of a failure of one controller or if stopped for maintenance purposes, control shall fail over to the standby controller in a single controller scan. High performance controllers shall provide a typical scan time, and hence failover time, of 5 to 20ms, depending upon the application.

RMX shall support multi-mode fiber up to 300 meters or single-mode fiber up to 10km. The fiber connection shall be direct and no additional fiber hubs or switches, or other hardware shall be required.

A dual synchronization link shall be provided to eliminate any single point of failure.

The synchronization module must be separate module for better availability and not embedded with the CPU

6 – Standalone Controllers for Simplex

General

Simplex, standalone controllers should support real-time application status, remote diagnostics and a range of communications protocols, including PROFINET. The PACSystems RSTi-EP CPE100 is an example of such a controller.

Packaging

All components shall be housed in structurally secure enclosures and should have ready-to-go functionality upon being unboxed.

Environmental Conditions

Edge controllers shall operate effectively in a temperature range of -40 to +70 °C.

Central Processing Unit

The CPU shall possess the capability to solve application logic, store the application program (including documentation of variable names, rung comments and documentation files), store numerical values related to the application processes and logic and interface to the I/O systems. The CPU shall need no additional modules to provide at least the following advanced programming features: floating point math, PID, modulo, math, double precision math, logical functions, subroutines, data array move and indirect addressing. The CPU shall contain a 1GHz TI AM335x Sitara SoC microprocessor or a microprocessor of equivalent capabilities.

Multi-Discipline Controller Environment

The controller shall be capable of supporting process, discrete and batch applications at the same time.

Physical Requirements

Interfaces

The controller should feature at least the following:

- Dual LAN interfaces with four Ethernet ports
- Built-in RS-232 serial port

Cooling Method

The controller should not include the use of any fans.

Dimensions

The controller should occupy just 1.5” (38.1mm) of DIN rail space.

7 – Rackless Controllers for High-Availability

General

The system shall consist of rugged components designed specifically for industrial environments. A complete system shall consist of CPUs and one or more racks containing I/O modules, interconnected by signal cables.

Packaging

All components shall be housed in structurally secure enclosures.

The controller CPU shall be a single, stand-alone module.

The CPU shall be fully enclosed in a metal covering protecting the electronic circuitry from exposure (IP20 protection).

Wherever possible, all assemblies and sub-assemblies performing similar functions shall be interchangeable.

The system design shall accommodate the replacement of assemblies without having to disconnect field wiring. Wherever possible, removable connectors shall be used to connect field wiring to the individual circuit board assemblies.

All major assemblies and sub-assemblies, circuit boards and devices shall be identified using permanent labels or markings, each of which indicates the manufacturer's catalog number, product manufacturing date code, UL and C-UL certifications.

Environmental Conditions

Rackless controllers shall meet the following environmental specifications.

Operating Environment:

Hazardous Area Location:	ATEX Eex nA IIC T4
Field wiring:	ATEX 3G Iic T4 –nL
Temperature:	-40 to +70 deg C (32 to 140 deg F)
Airborne Contaminants:	IAS-S71.04 – 1985 Airborne Contaminants Class G2

Storage Conditions:

Temperature:	-40 to 85 degrees Celsius

Operating Conditions:

Temperature:	-40 to +70 degrees Celsius
Humidity:	5 to 95% relative humidity, non-condensing

Central Processing Unit

The CPU offered shall be a stand-alone unit. The CPU shall possess the capability to solve application

logic, store the application program (including documentation of variable names, rung comments and documentation files), store numerical values related to the application processes and logic and interface to the I/O systems. The CPU shall need no additional modules to provide at least the following advanced programming features: floating point math, PID, modulo, math, double precision math, logical functions, subroutines, data array move and indirect addressing.

Rackless CPU

The rackless CPU shall contain: A minimum Intel or compatible microprocessor operating at speeds no less than 1 GHz as the main processing element, memory mounted on the board. A minimum of 64Mb of retentive user memory shall be on board for user configurable application, data storage and documentation storage. User memory will be backed up by built-in Flash memory of the same capacity as the user memory.

The rackless CPU shall contain a real-time calendar and clock that can be accessed by the user program. This Time of Day clock and calendar shall be battery-backed and maintain seven-time functions: year (2 digits), month, day of month, hour, minute, second and day of week.

The rackless CPU shall execute Boolean functions at a rate of 0.3 microseconds per instruction or lower.

The CPU shall provide Ethernet ports for communications. Ethernet shall be 10/100/1000Gbs^{-1} with four ports for separate connections. One port shall support PROFINET Controller functionality with a built-in switch and MRP protocol for PROFINET network redundancy. One port shall support optional synchronization for use in redundant systems. One port shall support interfacing to the cloud, see section entitled “IIoT: Industrial Internet Control System (IICS)”.

A RUN ENABLED/RUN DISABLED/STOP switch shall be supported by the CPU using a mechanism designed to prevent accidental selection of any mode.

An OLED display, supplemented by LEDs on the CPU, shall indicate the following:

- CPU OK
- RUN mode
- Outputs Enabled
- I/O Force
- System faults
- Communications activity
- IP address details
- Firmware version

Multi-Discipline Controller Environment

The controller shall be capable of supporting process, discrete and batch applications at the same time.

Cyber security

The controller CPU shall support the following

- Secure boot
- TPM (Trusted Platform Module)
- Secure firmware updates
- Multiple password-protected levels of access with increasing privileges
- Secure and encrypted communications
- Encrypted passwords
- Disabled unused network ports
- Throttling on Ingress/Egress communications on Ethernet ports
- Achilles Level 2 certified

Controller System Diagnostics

Visual Diagnostics

An OLED display, supplemented by LEDs on the CPU, shall provide a status display for the CPU.

Alarm Processor

The CPU shall contain an alarm processor that is special process controller feature designed to receive and process faults. The diagnostics shall provide information on the configuration and CPU, memory, communications and I/O status.

The alarm processor function shall log I/O and system faults in two fault tables that shall be accessible for display on the PC compatible programming software screen or uploaded to a host computer or other coprocessor.

The alarm processor shall maintain the states of up to 128 discrete system diagnostic bits to be read by a host or incorporated as contacts into the ladder program for customized diagnostic routines.

Each fault table shall have a total capacity of 32 faults. The last 16 entries shall maintain the latest 16 faults. The first 16 shall be kept unchanged.

Faults may be cleared by the user by way of a programmer. Provision shall be made by way of passwords to protect these faults from unauthorized clearing.

Alarm Features

The alarm processor shall report three types of fault action; fatal, diagnostic, or informational and the CPU shall respond as follows:

Faulty Action	Fatal	Diagnostic	Informative
CPU Enters STOP Mode	Yes	No	No
Set Diagnostic Bit	Yes	Yes	No
Logged In Fault Table	Yes	Yes	Yes

When an I/O fault occurs, the alarm processor shall report the drop, rack and slot location of the fault, the condition, the address and the circuit number if appropriate.

This alarm processor function shall have the capability to time-stamp system faults for future references.

CPU Memory

Memory Capacity

The process controller shall supply a rackless design CPU that contains at least the following:

- 64 Megabytes for application programming
- Configurable up to 4Mb 16-bit registers for register and data usage
- Up to 32K control relays internal battery backed
- Up to 32K bits for discrete inputs
- Up to 32K bits for discrete outputs
- Configurable up to 32K 16-bit registers for analog inputs
- Configurable up to 32K 16-bit registers for analog outputs

All application memory shall be available to the user program. Executive level operations performed by the CPU shall not consume application memory.

Memory Storage

The register values and the application program shall be stored in battery-backed SRAM. The application program and system configuration shall also be stored in FLASH memory if so selected.

There shall be an energy pack of capacitors used to maintain the contents of the RAM memory in the CPU. The energy pack shall be replaceable with power applied to the process controller and without removing the CPU. Batteries, except for small coin-cell types, shall not be used to avoid explosion and fire risk and to eliminate issues with shipping of equipment.

There shall be an easy connection for the energy pack to connect and be replaced while running.

An LED shall provide visual indication of the energy pack condition. Additionally, poor energy pack condition shall be alarmed with a system diagnostic bit.

The CPU shall allow resident user program to be maintained in the CPU without power applied. A CPU shall be able to be shipped without energy pack battery connected and the user program and data

registers preserved in Flash memory.

The CPU shall calculate the application program checksum at the end of every sweep. A complete checksum calculation for a program may take several sweeps. A fixed number of program memory checksum shall be calculated each sweep. This number is configurable by the user. If the calculated checksum does not equal the reference checksum, a fault shall be recorded, and the CPU mode will change to STOP.

The memory on the CPU shall be capable of storing support documentation such as Word, Excel, CAD and other files in RAM and FLASH.

Redundancy Synchronization and Failover

The rackless controller shall support high speed redundancy synchronization and failover using an Ethernet-based synchronization network. The controllers shall be synchronized frequently. In the event of a failure of one controller or if stopped for maintenance purposes, control shall fail over to the standby controller within at least 300ms, depending upon the application.

The Ethernet-based synchronization network shall support standard copper Ethernet cables up to 100 meters. The cable connection shall be direct and no additional hubs or switches or other hardware shall be required. Additional hubs or switches or other hardware may be used to allow extended distance between controllers of up to 10km.

A dual synchronization link shall be provided to eliminate any single point of failure.

8 – Edge Controllers

IICS: Edge Controller

The vendor shall provide an Edge controller and support for an Industrial Internet Control System (IICS) secure solution. This includes storage, analysis and rapid conveyance of data from the Edge of industrial systems.

The IICS PACSystems RX3i CPL 410 is an example of an approved Edge Controller that allows an approved application to rapidly adapt to changing business objectives. The Edge Controllers must leverage analytics to augment real-time control with external intelligence delivered through market analysis, fleet and enterprise, data, and asset/process knowledge. An Edge Controller should allow analysis to improve even a complex application at the source and/or push to the cloud or enterprise using connected services.

The Edge Controller shall comprise of a real-time control engine and PACEdge running in a hypervisor environment. The hypervisor will support running two or more operating systems on the same processor using multiple cores with one or more cores dedicated to each operating system. System resources such as network ports shall be securely allocated to one operating system as required. The hypervisor should provide secure operation of each operating system with no adverse interaction at the hardware level – the non-real time operating system may be shut down and re-started with no impact on the other operating system.

Different families of operating system running at the same time should be supported, for example running Linux alongside a real-time operating system such as VxWorks. The hypervisor will maintain a virtual Ethernet port between operating systems to support communication where required using protocols such as OPC UA.

Edge Controllers should be ruggedized for uninterrupted data collection, reliable performance, and customizable to fit almost any application.

The capabilities of the Edge Controller shall be as outlined in the section below.

General

The Edge Controller shall implement OS level virtualization for deterministic real-time control and an open edge compute platform all in the same rugged, secure by design hardware platform. The PACSystems RX3i CPL410 is an example of such a controller.

The Edge Controller shall provide a single, secure platform for both IEC-61311 programming and open-source Linux applications and programming such as Python and JavaScript.

The Edge Controller shall provide a secure environment for adding open-source IIoT capabilities onto the control platform enabling real-time analytics, web-based visualization, and/or secure connectivity to the enterprise or cloud. Supporting the installation of tools such as, Node-Red, Grafana, Docker, InfluxDB and the numerous other of software available in the open source community.

Out of the box supported capabilities should include; webserver with SSL, database, secure OPC UA client, and Python script interpreter.

A firewall shall be implemented between the real time operating system and the open edge compute platform limiting denial of service attacks over Internet Control Message Protocol (ICMP) and restricting access to limited, securable protocols. This firewall shall not be modifiable from any application, further limiting the attack surface.

Packaging

All components shall be housed in structurally secure enclosures and should have ready-to-go functionality upon being unboxed. The controller should be stand alone with DIN rail and surface mount hardware available in the packaging.

Environmental Conditions

Edge controllers shall meet the following environmental specifications.

Operating Environment:

ATEX Directive:	Category 3 equipment [II 3 G]
	EN 60079-0: 2012 A+11:2013
	EN 60079-7: 2015 [Type of Protection Ex ec]
Temperature:	-40 to +70 °C
Humidity:	5 to 95% relative humidity, non-condensing
Certifications:	UL HAZLOC C1D2, ATEX Zone 2, ABS, BV, DNV, GL

Central Processing Unit

The CPU shall possess the capability to solve application logic, store the application program (including documentation of variable names, rung comments and documentation files), store numerical values related to the application processes and logic and interface to the I/O systems. The CPU shall need no additional modules to provide at least the following advanced programming features: floating point math, PID, modulo, math, double precision math, logical functions, subroutines, data array move and indirect addressing. The CPU shall contain a 1.2GHz AMD (4-Core) microprocessor.

Multi-Discipline Controller Environment

The controller shall be capable of supporting process, discrete and batch applications at the same time.

Cyber security

The controller CPU shall support the following

- Secure boot
- TPM (Trusted Platform Module)
- Secure firmware updates
- Multiple password-protected levels of access with increasing privileges
- Secure and encrypted communications

- Encrypted passwords
- Disabled unused network ports
- Throttling on Ingress/Egress communications on Ethernet ports
- Redundant controller shall be Achilles Level 2 certified

Physical Requirements

Visual Diagnostics

LEDs on the CPU shall provide a status display for the CPU.

Cooling Method

The controller should rely on the use of heat sinks for cooling and avoid any use of fans.

Dimensions

The controller should be 168 x 57.6 x 161.5 (mm) in size.

Redundancy Synchronization and Failover

The controller shall support built-in high-availability with hot-standby controller redundancy.

9 – I/O Systems

General

The system shall consist of rugged components designed specifically for industrial environments. A complete system shall consist of one or more racks containing I/O modules, interconnected by signal cables. Figure 9.1 below provides a summary of the I/O families that are available for use with PACSystems* RX3i PROFINET System Redundancy (PNSR) applications.

							
Product	**PACSystems RSTi**	**PACSystems RSTi-EP**	**VersaPoint/ VersaSafe**	**VersaMax Modular**	**VersaMax/IP**	**PACSystems RX3i**	**PAC8000**
Mounting Format	DIN Rail	DIN Rail	DIN Rail	DIN Rail	On Panel/Machine	On Panel/DIN Rail	DIN Rail
Network Interfaces	PROFINET PROFIBUS DP Modbus/TCP	PROFINET PROFIBUS DP Modbus/TCP	PROFINET PROFIBUS DP Modbus/TCP	PROFINET PROFIBUS DP Modbus/TCP	PROFINET PROFIBUS DP	PROFINET PROFIBUS DP Modbus/TCP	PROFINET Modbus/TCP
Gateways/Bridges	Serial Communications	Serial Communications IO Link	Serial Communications	Modbus/RTU PROFIBUS Master	None	Serial Communications PROFIBUS/Master CANOpen Modbus/RTU Modbus/TCP HART GENIUS DNP3 Serial/TCP IEC-61850 IEC-104 Reflective Memory	HART
Network Redundancy	None	MRP	MRP	MRP	MRP	MRP, Dual LAN	MRP, Dual LAN
System Redundancy	None	PNSR	None	PNSR, EGD or GENIUS	None	PNSR, EGD or GENIUS	PNSR[1] or MBus/TCP
IO Redundancy	None	Via Application Code	None	Via Application Code	None	Via Application Code	Dual
Media Support	Copper	Copper	Copper & MM Fiber	Copper & MM Fiber	Copper	Copper, MM & SM Fiber	Copper & MM Fiber
Media Connector	2x RJ45	2x RJ45	2x RJ45 or 2x SCRJ	2x RJ45 or 2x ST	2x M12	2x RJ45 + 2x SFP	2x RJ45 or 2x ST
I/O Type	TTL, 12, 24, 48, 125 VDC 120, 240 VAC, relay, analog, RTD, Thermocouple	24, 125 VDC 120, 240 VAC, relay, analog, RTD, Thermocouple	24 VDC Relay analog, RTD, Thermocouple	TTL, 12, 24, 48, 125 VDC 120, 240 VAC, relay, analog, RTD, Thermocouple	24 VDC analog	TTL, 12, 24, 48, 125 VDC 120, 240 VAC, relay, analog, RTD, Thermocouple	24 VDC, 115, 230 VAC in 2-60 VDC, 20 - 265 VAC out analog, RTD, Thermocouple
Speciality Modules	High Speed Counters SSI Interface PWM and Pulse Output	High Speed Counters SSI Interface PWM and Pulse Output Power Measurement SIL3 Power Feed IO Link	High Speed Counters SSI Interface Absolute Encoder Motor Starters SIL3 Logic Processor SIL3 24 VDC, SIL3 relay	High Speed Counters PWM and Pulse Output	None	Pulse Test 24, 125 VDC High Speed Counters PWM and Pulse Output Power Sync & Measure Strain Gauge SoE Inputs (application)	Pulse Test 24 VDC Pulse Input SoE Inputs ASH Detector
Isolation	None	Galvanic Isolation AC DI	None	Galvanic Isolation DI, DO, AI, AO	None	Galvanic Isolation DI, DO, AI, AO	Galvanic Isolation DI, DO, AI, AO
Hot Swap	No	Yes	No	Yes	No	Yes	Yes
Environmentals	IP20 0 to 55C (UL) 0 to 60C (non-UL)	IP20 -20 to 60C	IP20 -20 to 55C	IP20 0 to 60C opt -40 to 60C opt Conf Coat	IP67 -20 to 60C	IP20 0 to 60C opt -40 to 60C opt Conf Coat	IP20 -40 to 70C Conf Coat
Agency Approvals	UL, UL HAZLOC C1D2 CE, ATEX Zone 2	UL, UL HAZLOC C1D2 CE, ATEX Zone 2 TUV SIL3 GL	UL, UL HAZLOC C1D2 CE, ATEX Zone 2 TUV SIL3	UL, UL HAZLOC C1D2 CE, ATEX Zone 2 ABS, BV, DNV, GL, LR	UL, UL HAZLOC C1D2 CE	UL, UL HAZLOC C1D2 CE, ATEX Zone 2 ABS, BV, DNV,GL, KRS, LR	UL, UL HAZLOC C1D1 CE, ATEX Zone 1, IS TUV SIL2 LR, G3
Channel Density	1 - 16 points	4 - 16 points	1-8 points	4-32 points	4,8 points	2-32 points	2-32 points
Max Wire Gauge	16	16	16	14	M12	12 (low density) 14 (high density)	14
Max I/O per Drop	512	1024	400	1024	128	448	1024
I/O Module Size	12mm W x 99mm H x 70 mm D	11.5mm W x 120mm H x 76mm D	12mm W x 120mm H x 70 mm D	66.8mm W x 163.5mm H x 70 mm D	70 mm W x 178 mm H x 49.3 mm D	34mm W x 145mm H x 140 mm D	42mm W x 110mm H x 106 mm D

Figure 9.1 Emerson I/O Product Portfolio Summary

The sections below specifically describe the chassis based remote IO capability of RX3i IO.

Packaging

All components shall be housed in structurally secure enclosures.

The I/O system shall be modular. Each module shall be fully enclosed within a durable plastic or metal shroud. When mounted on the system base, each I/O module shall not occupy more than one available slot. Mechanical anchor points shall be part of the module for securing field wiring.

There shall be at least five sizes of base available, supporting 1, 2, 7, 12 and 16 modules. The base shall support a high-speed serial bus and a high-speed PCI bus.

I/O modules shall be retained in their slot by a hinge on the upper rear edge and snap on the lower rear edge of the baseplate. Any module without metal housings should be able to be inserted and removed without the use of tools. Modules with metal housings should be able to be inserted and removed with simple hand tools.

I/O modules shall be installed in any available slot in the CPU or expansion baseplates.

I/O modules shall connect electrically to the baseplate via a pin and socket connector.

I/O modules shall be fully enclosed in a plastic covering protecting the electronic circuitry from exposure (IP20 protection).

Base shall include an integrated grounding bar at the bottom of the base for securing shields and commons from field devices to minimize noise into the modules.

Wherever possible, all assemblies and sub-assemblies performing similar functions shall be interchangeable.

The system design shall accommodate the replacement of assemblies without having to disconnect field wiring. Wherever possible, removable connectors shall be used to connect field wiring to the individual circuit board assemblies.

All major assemblies and sub-assemblies, circuit boards and devices shall be identified using permanent labels or markings, each of which indicates the manufacturer's catalog number, product manufacturing date code, UL and C-UL and CE certifications.

Environmental Conditions

I/O components of the controller system shall meet the following environmental specifications:

Operating Environment:

Hazardous Area Location:	ATEX Eex nA IIC T4
Field wiring:	ATEX 3G Iic T4 –nL
Temperature:	0 to 60 deg C (32 to 140 deg F)
Airborne Contaminants:	IAS-S71.04 – 1985 Airborne Contaminants Class G2

Storage Conditions:

Temperature: -40 to 85 degrees Celsius

Operating Conditions:

Temperature: 0 to 60 degrees Celsius

Humidity: 5 to 95% relative humidity, non-condensing

A low temperature testing service shall support operation from -40 to 60 degrees Celsius.

Some components shall support extended temperature operation of -40 to +70 degrees Celsius.

Discrete I/O

Modularity

Interface between the process controller and user supplied input and output field devices shall be provided by rack-type I/O modules.

Configuration

There shall be an expandable system.

Ethernet expansion racks shall be connected via a 10/100/1000Mbs Ethernet, RJ-45 connection, using the PROFINET protocol. Fiber connection shall also be supported. The PROFINET Controller (PNC) interface unit shall reside in the rack using the same I/O that is compatible with the controller or be embedded into the CPU. The PNC shall support the following.

- Built-in switch to allow daisy chain connection to the next device.
- Support redundant controllers with automatic switch over.
- Support a fault tolerant ring architecture using Media Redundancy Protocol (MRP)
- Support redundant I/O using PROFINET System Redundancy (PNSR)

I/O Addressing

I/O reference addressing for each I/O module shall be assigned through the use of the PC-compatible configuration and programming software. There shall be no jumpers or DIP switch settings required to address modules.

The circuit status of each I/O point on a module shall be indicated by a green LED mounted at the top of the module. These LEDs must be visible through a clear plastic lens. Each LED shall illuminate a letter and number which corresponds to the energized I/O circuit.

Addressing of all references including I/O must be represented as a decimal-based number.

Construction

Terminal blocks shall be easily removable and common to all discrete and analog I/O to allow for convenient pre-wiring of field devices.

Each I/O module shall contain a hinged, clear plastic, terminal block cover (door) with a removable label.

The inside of the label shall have the module description, catalog number and circuit wiring diagram for that module type and the outside of the label shall have a user legend space to record circuit identification information.

The label shall have color coding for quick identification of the module as high voltage (red), low voltage (blue), or signal level (gray) type.

Input Specifications

The 120 Volt AC input module shall accommodate an input voltage range from 0 to 132 volts.

The 240 Volt AC input module shall accommodate an input voltage range from 0 to 264 volts.

The 24 Volt DC positive and negative logic input modules shall accommodate an input voltage range of 0 to +30 volts DC.

The 125 Volt DC input module shall accommodate an input voltage range from 0 to 150 volts.

Availability of Input Modules

As a minimum, the following discrete input modules shall be available:

Description	Points/Module
Input Simulator	8, 16
120 Vac Isolated Input	8, 16
240 Vac Isolated Input	8
120 Vac Input	16, 32
48 Vdc Positive/Negative Logic Input	16
24 Vac/Vdc Negative Logic Input	16
24 Vdc, Positive/Negative Logic Input	8, 16, 32
24 Vdc Positive/Negative Logic Input, (1ms response)	16
125 Vdc Positive/Negative Logic Input	8
5/12 Vdc Positive/Negative Logic Input (TTL)	32

Output Specifications

Discrete AC output modules shall have separate and independent commons, allowing each group to be used on different phases of AC supply.

Each discrete AC output shall be provided with an RC snubber to protect against transient electrical noise on the power line.

Discrete AC outputs shall be suitable for controlling a wide range of inductive and incandescent loads by providing a high degree of inrush current (10x the rated current).

Discrete DC output modules shall be available with positive and negative logic characteristics in compliance with the IEC industry standard.

Discrete DC output modules shall be provided with at least eight output points in a group with a common power input terminal per group.

Discrete DC output modules shall be compatible with a wide range of user-supplied load devices, such as: motor starters, solenoids and indicators.

A 2 Amp relay output module shall be capable of supplying 2 Amps resistive maximum load per output and 4 amps resistive maximum load per group of 4 outputs.

A 4 Amp relay output module shall have 8 isolated outputs per module and shall be capable of supplying 4 amps resistive maximum load per output and 32 amps resistive maximum load per module.

Availability of Output Modules

As a minimum, the following discrete output modules shall be available:

Description	Points/Module	Fuse Rating	# Fuses/Module
120 VAC, 0.5A (2 groups)	12, 16	3A	2
120/240 VAC, 1A (2 groups)	8	3A	2
120/240 VAC Isolated, 2A	5	3A	5
48VDC Positive Logic, 0.5A	8	0.5A	2
12/24 VDC Positive Logic, 2A	8	5A	2
12/24 VDC Positive Logic, 0.5A	8, 16, 32	N/A	0
12/24 VDC Negative Logic, 2A	8	5A	2
12/24 VDC Negative Logic, 0.5A	8, 16	N/A	0
125 VDC Positive/Negative Logic, 1A	6	N/A	0
5/12/24 Vdc Negative Logic, 0.5A	32	N/A	0
Relay, Normally Open, 2A (4 groups)	16, 24	N/A	0
Relay, Normally Open, 4A Isolated	8, 16	N/A	0
Relay, Isolated, 4 Normally Closed,	8	N/A	0
Relay Normally Open (Form B & C) 8A	8	N/A	0

Availability of Mixed I/O Modules

As a minimum, the following discrete output modules shall be available:

Description	Points/Module
24 Vdc Input, Relay Output	8 in, 8 out
120 Vac Input, Relay Output	8 in, 8 out

Analog I/O

General Specifications

For the conversion of analog to digital and digital to analog conversion required by an application, the following shall be available.

Analog Voltage Input

The analog voltage input module shall be capable of converting 8 or 16 channels of inputs in the range of 0 to 20mA, 4 to 20mA, 0 to 5 volts, 1 to 5 volts, -5 volts to 5 volts, 0 to 10 volts and -10 to +10 volts. Each channel is configurable.

An 8-channel analog input module shall be available to support on a per-channel basis any combination of the following:

- Thermocouple Inputs: B, C, E, J, K, N, R, S, T
- RTD Inputs: PT 385 / 3916, N 618 / 672, NiFe 518, CU 426
- Resistance Inputs: 0 to 250 / 500 / 1000 / 2000 / 3000 / 4000 Ohms
- Current: 0–20mA, 4–20mA, ±20mA
- Voltage: ±50mV, ±150mV, 0–5V, 1–5V, 0–10V, ±10V

Resolution of the converted analog voltage input signal shall be 16 bits binary.

All of the channels of converted analog voltage input signals shall be updated each scan into a dedicated area of data registers in a 16-bit 2's complement format.

The conversion speed for all of the analog input channels shall be configurable via filtering from 14ms and no greater than 490ms.

The module shall support the following diagnostics:

- Open-circuit detection
- High alarm, low alarm, high-high alarm, low-low alarm detection and reporting
- Positive and negative rate of change alarms
- Module fault reporting
- Configurable CPU interrupts for channel alarms and faults
- Supports diagnostic point fault contacts in the logic program.

The module shall support user-defined scaling.

Analog Voltage Output

The analog voltage output module shall be configurable per channel to be capable of converting 4 or 8 channels of digital data to analog outputs in the range of 0 to 10 volts, -10 to +10 volts, 0 to 20ma and 4 to 20ma.

Resolution of the converted output signal shall be 16 bits.

All channels of analog output data shall be updated each scan from a dedicated area of data registers in a 16-bit 2's complement format.

The analog output module shall support clamping to prohibit invalid control ranges. Configurable to Hold Last State or Output Defaults

Ramp rate option for normal operation and during fault operation.

Analog Combination

The analog combination module shall be capable of converting 4 channels of analog inputs to digital data and 2 channels of digital data to analog outputs.

All channels are configurable for 0-20ma, 4-20ma, 0-+10V and -10-+10V. Resolution of the converted input signals shall be 12 bits and output signals shall be 16 bits.

All channels of analog data shall be updated each scan from a dedicated area of data registers in a 16-bit 2's complement format.

The analog outputs shall be configurable to default to 0 volts or hold-last-state in the event of a CPU failure.

Module Availability

As a minimum, the following analog modules shall be available:

Description	Channels/Module
Voltage/Current	8, 16
Voltage Analog Input	4, 16
Voltage/Current Input	8, 16
Voltage/Current Output	4, 8
Current Analog Output	2, 8
Voltage Analog Output	2, 8
Universal Analog In V, C, RTD, TC, Strain	8
Combo Analog Inputs/Outputs	4/2

Intrinsically Safe (IS) I/O

General

In addition to the I/O requirements highlighted in this section, the vendor the vendor shall offer an option

for Intrinsically Safe (IS) I/O to work with PACSystems solutions. This IS I/O is to have IS isolation built-in to the I/O devices, with no external barriers or additional IS components required. The IS I/O shall be suitable for mounting in a zone 2 area with the I/IO in a zone 1 area.

Analog Input Types

The IS I/O should have the following analog input module types available:

- Thermocouple Inputs: B, E, J, K, N, R, S, T, W3, W5, Russian K, Russian L
- RTD Inputs: Pt100, Pt500, jPt100, Ni120
- Resistance Inputs: 0 to 110 / 280 / 470 / 2000 Ohms
- Current: 4–20mA

Modularity

Interface between the process controller and user supplied input and output field devices shall be provided by rack-type I/O modules.

Configuration

There shall be an expandable system.

Ethernet expansion racks shall be connected via RJ-45 connection using either Modbus or PROFINET protocols. Fiber connection shall also be supported for PROFINET modules. The PNS shall support the following.

- Built-in switch to allow daisy chain connection to the next device.
- Support redundant controllers with automatic switch over.
- Support a fault tolerant ring architecture using Media Redundancy Protocol (MRP)
- Support PROFINET System Redundancy (PNSR)

I/O Addressing

I/O reference addressing for each I/O module shall be assigned through the use of the PC-compatible configuration and programming software. There shall be no jumpers or DIP switch settings required to address modules.

The circuit status of each I/O point on a module shall be indicated by a green LED mounted at the front of the module. These LEDs must be visible through a clear plastic lens.

Addressing of all references including I/O must be represented as a decimal-based number.

Construction

Terminal blocks shall be easily removable and common to all discrete and analog I/O to allow for convenient pre-wiring of field devices.

Input Specifications

Availability of Input Modules

As a minimum, the following discrete input modules shall be available:

Description	Points/Module
Analog, 4–20 mA with HART	8
Analog, 4–20 mA	8
Analog, 1-5V	8
Discrete, 24 V dc, isolated, sinking	8, 16
Discrete, 24 V dc, non-isolated, module powered	8. 16
Discrete, non-isolated, powered inputs and outputs	8
Discrete, 115 V ac, isolated, sinking	8
Discrete, 115 V ac, non-isolated, module powered	8
Discrete, 230 V ac, isolated, sinking	8
Discrete, 230 V ac, non-isolated, module powered	8
Discrete, 115 V ac, block-isolated, sinking	16
Discrete, Switch/Proximity Detector Inputs, Module Powered	32
Pulse, 2-channel, pulse/quadrature input	2

Output Specifications

Availability of Output Modules

As a minimum, the following discrete output modules shall be available:

Description	Points/Module
Analog, 4–20 mA with HART	8
Analog, 4–20 mA	8
Discrete, 2–60 V dc, non-isolated, module powered	8
Discrete, 20–265 V ac, non-isolated, module powered	8
Discrete, 2–60 V dc, isolated, unpowered	8
Discrete, 20–265 V ac, isolated, unpowered	8
Discrete,12-42 V dc, non-isolated, module powered	16

HART

General

In addition to the I/O requirements highlighted in this section, the vendor the vendor shall support HART functionality to communicate with sensors. The objective of this functionality is to provide an earlier

insight to device data and add smarter diagnostics for preventive maintenance.

“HART-ability”

The vendor shall offer solutions that provide connections between HART field instruments, the control systems, and the process automation maintenance software. Specifically, it shall allow the host control software and any HART field instruments to communicate directly with each other. In addition, HART connection systems will provide on-line access from a PC to the HART field devices for monitoring device performance. HART devices may be selected for regular status monitoring and alerts can be issued if the status changes.

HART Modules

All modules with HART capabilities should be able to can obtain information from HART instruments of protocol revision 5.0 or later. Each channel shall allow communication with a single HART instrument. HART universal command 3 should be used to gather up to 4 dynamic variables and status from each HART instrument. In addition, HART pass-through may be used for device configuration, calibration and advanced diagnostics. Any digital HART data should be stored in its original IEEE754 floating point format.

Specialty Modules

High Speed Counter Modules

A specialized high-speed counter (HSC) option module shall be available to accommodate applications where pulse input rates exceed the input capability of the controller.

The high-speed counter module shall provide direct processing of rapid pulse signals up to 1.5MHz in frequency.

The high-speed counter module shall be configurable as four or eight independent counters counting either up or down, two independent bi-directional counters, or one counter that can calculate the difference between two changing count values.

Power Synchronization and Measurement Module

A specialized power synchronization and measuring (PSM) option module shall be available to accommodate applications where power monitoring and synchronization of power generation systems is required.

The power synchronization and measuring module shall provide direct processing of electrical parameters including voltage, current, power (active and reactive), frequency, phase angle and support waveform capture for harmonic analysis. The module shall support data collection for two separate power networks and allow comparison of the two systems with isolated outputs to provide synchronization capability when the networks are within specified limits.

An interface module shall be provided to support direct connection to systems up to 750Vac with current transformer (CT) connection for all current measurements. Potential transformer (PT) connection shall be supported for higher voltage systems.

The power synchronization and measuring module shall provide calculation of ANSI-standard

parameters including under-voltage, reverse power, negative sequence, over-current, over-voltage, voltage/current imbalance and under- and over-frequency.

The power synchronization and measuring module shall support connection to single- and three-phase networks. For three-phase networks, wye and delta power systems shall be supported.

I/O Time Stamping

The I/O Time Stamping feature allows the user to specify which discrete input channels within a Remote I/O station node should be time stamped when rising edge (0→1), falling edge (1→0), or either type of transition occurs. The high-resolution timestamp will contain an epoch number, seconds, and nanoseconds, and, will be correlated to a common time base. As events occur, the Remote I/O station automatically places them into a local event buffer, which are periodically transitioned to an even recorder for the system. This feature is often implemented as a Sequence of Events (SoE) recorder to assist with root-cause analysis in complex control applications. Events collected at Remote I/O stations will be relayed to a central event recorder either periodically or by application request for archival and subsequent review in the event of a failure in the application.

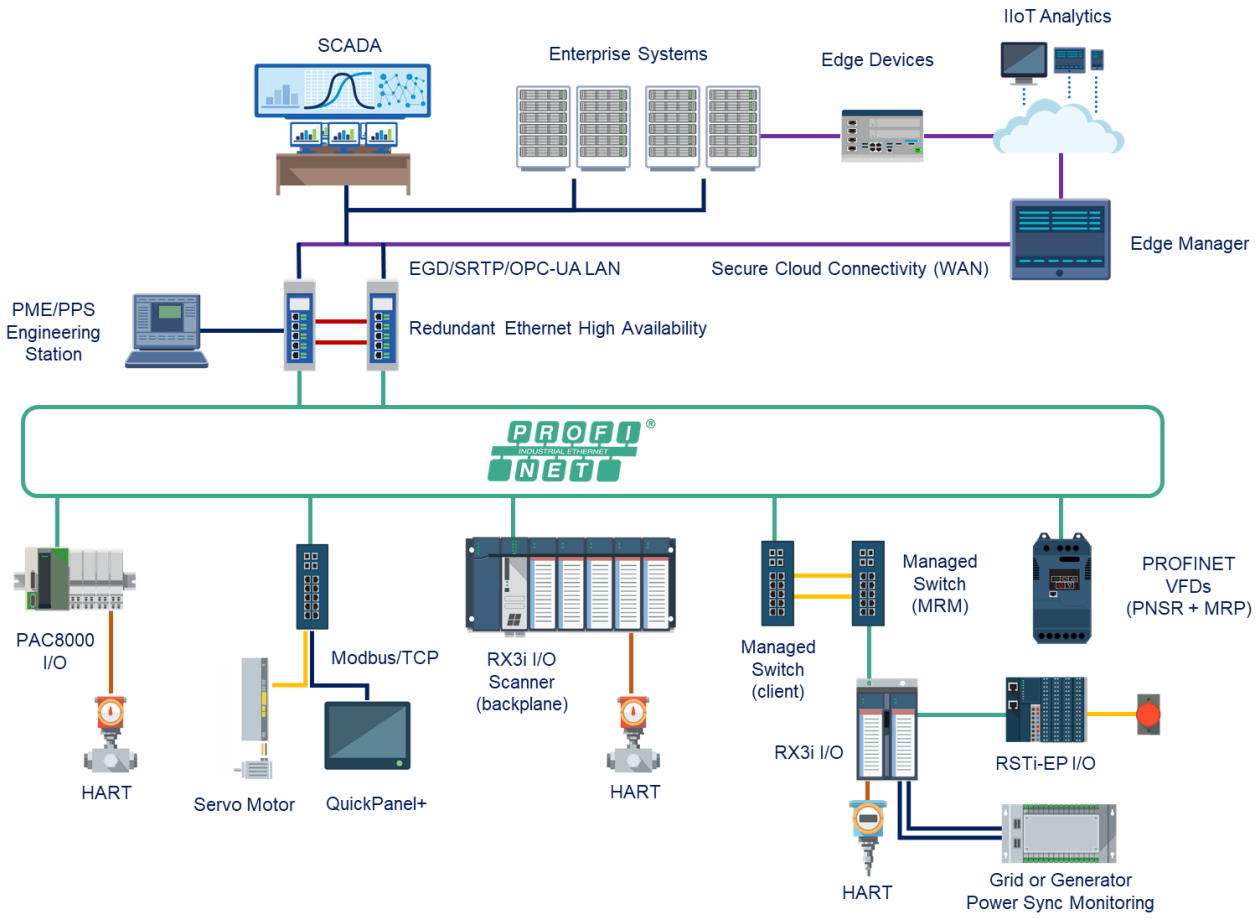


Figure 9.2 System Architecture for Small-to-Midsize Applications with I/O Time Stamping

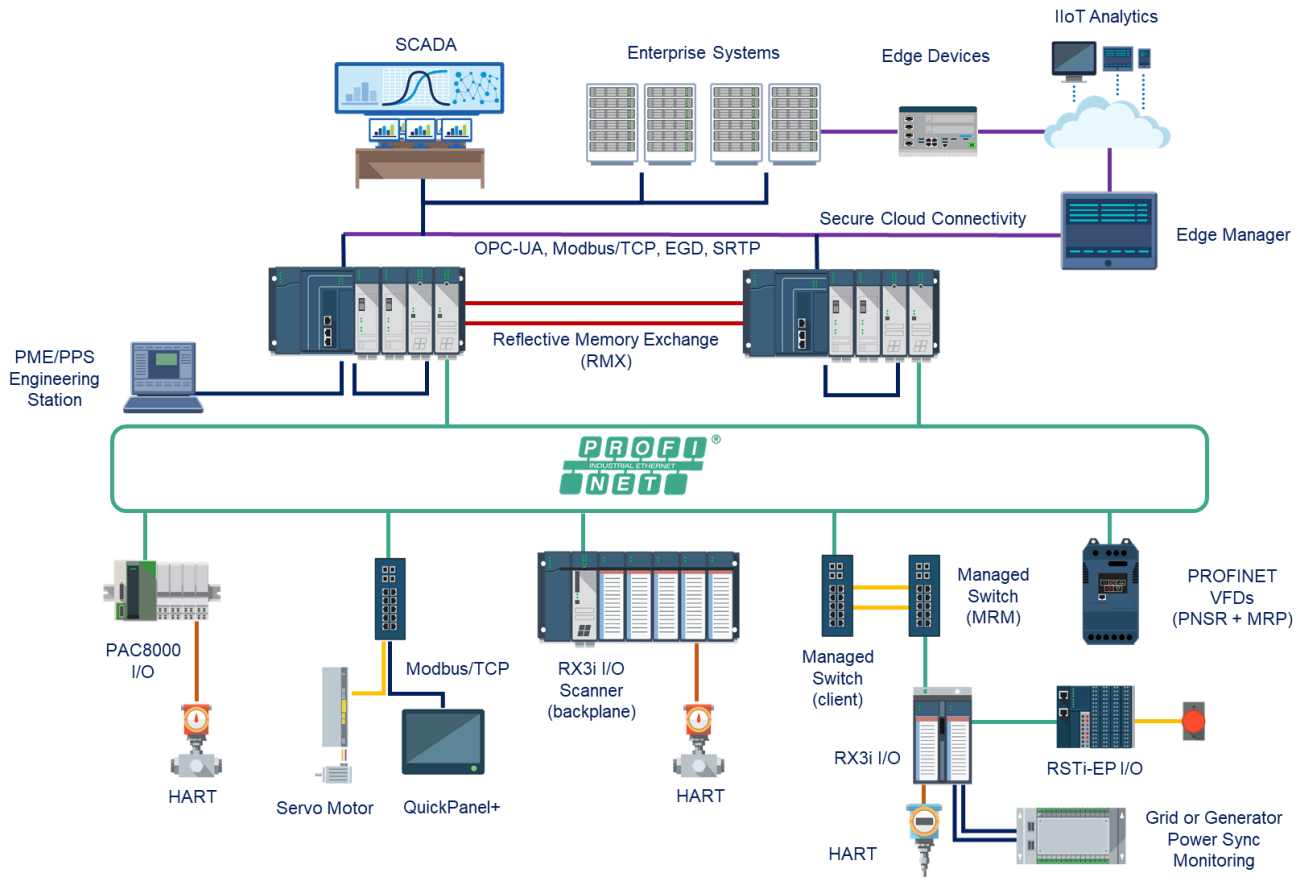


Figure 9.3 System Architecture for Midsize-to-Large Applications with I/O Timestamping

Time Synchronization Protocols

The control system shall support time stamping using the following protocols for distribution of the common time base. The listed accuracy shall be possible with the given protocol between points within a single I/O module, within a remote I/O station, and between remote I/O stations.:

SNTP – 3 milliseconds

IRIG-B – 1millisecond

I/O Time Stamping Station

Remote I/O stations shall maintain direct connection or networked connection to a common time base with a local clock accuracy of at least 10 microseconds. If using a networked connection, all network switch equipment between the common time base and the remote I/O station shall support the utilized time synchronization protocol.

Remote I/O stations shall implement time stamping of up to 128 discrete inputs per station with an accuracy of at least 1 ms between points within a single I/O module, within a station, or between stations.

Remote I/O stations shall at a minimum allow for configuring discrete inputs of the following types:

- 5 VDC
- 12 VDC
- 24 VDC
- 48 VDC
- 125 VDC
- 120 VAC
- 240 VAC

Remote I/O stations shall have internal event buffering for at least 4096 events.

Remote I/O stations shall be capable of sustained reporting of at least 400 events/second

Event Recorder

The event recorder can exist either inside the redundant controllers or as a standalone processor on the I/O network. The event recorder shall maintain direct or networked connection to a common time base with a local clock accuracy of at least 10 microseconds.

The event recorder shall connect to up to 32 Remote I/O stations at a time

The event recorder shall be capable of recording events for up to 4096 discrete inputs.

The event recorder shall be capable of recording events at a rate of at least 400 events/second per Remote I/O station.

The event recorder shall be capable of recording events at a rate of at least 12,800 events/second per system.

10 – Industrial Switches

General

A range of industrial switches shall be available to extend the capabilities of the system, enhance maintainability, and provide critical machine-to-machine information. The switches shall work with Ethernet LAN and be designed to support suitable features in industrial applications.

Industrial Ethernet Switch Types

The vendor shall provide industrial Ethernet switches which cover the following applications:

- Standalone devices
- Connected devices
- Unmanaged switches
- Fully managed switches
- Rack mounted [Layer 3] switches
- PROFINET switches

Packaging

Switches shall be housed in structurally secure enclosures.

Switches shall be a single, stand-alone module.

Switches shall be fully enclosed in a metal covering protecting the electronic circuitry from exposure (IP30 protection).

Switches shall be either DIN-rail or rack mounted.

Wherever possible, all assemblies and sub-assemblies performing similar functions shall be interchangeable.

The system design shall accommodate the replacement of assemblies without having to disconnect field wiring. Wherever possible, removable connectors shall be used to connect field wiring to the individual circuit board assemblies.

All major assemblies and sub-assemblies, circuit boards and devices shall be identified using permanent labels or markings, each of which indicates the manufacturer's catalog number, product manufacturing date code, UL and C-UL and CE certifications.

Environmental Conditions

Switches shall meet the following environmental specifications:

Storage Conditions:

Temperature: -40 to 85 degrees Celsius

Operating Conditions:

Temperature:	-40 to +70 degrees Celsius
Humidity:	5 to 95% relative humidity, non-condensing

Performance and Connectivity

Switches shall support 10/100Base-T or 10/100/1000Base-T connections in a range of configurations including 4, 5, 6, 8, 10, 16 and 24 ports.

Switches shall offer an option for 100Base-FX or SFP ports for connection to a fiber backbone (multi-mode or single-mode).

Switches shall be available as unmanaged (layer 2) or managed (layer 3). Managed switches shall support a web interface for configuration. Network management software shall allow the network administrator to manage centralized configuration, visualize management and complete network monitoring with an early warning system, ensuring a stable and reliable industrial network

Reliability

Switches shall support redundant 12-45Vdc power supply connections to enhance overall system availability.

A wide temperature range shall be offered to support long life in harsh environments.

Monitoring

Switches shall support a relay output for fault event alarming.

Switches shall support a syslog server / client to record and view events, including SMTP for event warning notification via email.

Redundant Ring

Where used, switches shall support STP/RSTP/MSTP (IEEE 802.1D/w) Redundant Ring with recovery time less than 10ms over 250 units.

Security

Managed switches shall support the following security features.

- Device binding
- Enable/Disable ports
- MAC based port security
- Port-based network access control (802.1x)
- Support Q-in-Q VLAN for performance & security to expand the VLAN space
- VLAN top segregate and secure network traffic

- RADIUS centralized password management
- SNMP v 1/v2c/v3 encrypted authentication and access security
- DOS/DDOS auto-prevention
- Web and CLI authentication and authorization for web configuration interface

PROFINET Capabilities

The vendor shall offer switches that include PROFINET capability including the following.

- MRP support for PROFINET fault tolerant ring implementation.
- Support for redundant controllers using PNSR.
- Configure and diagnose from a single controller or redundant controller pair using a PROFINET IO device profile with GSDML file for import into controller configuration software.

Additional Capabilities

The vendor shall offer a wider range of network devices including wireless and GPRS/GSM modems.

11 – Security

Cyber Security

The system shall be as secure as possible at the cyber security level, including the following.

- Achilles testing/certification for controllers (ideally certification to level 2)
- Signed and encrypted firmware updates
- Security testing by independent security authority
- Application security provision
- Computer network data encryption where performance allows
- Secure development process
- Facility to alert vendor of security issues
- Notification system to advise users of issues and allow updates to be distributed

Advanced Cyber Security Features

Trusted Platform Module (TPM) v2.0

A secure cryptoprocessor/TPMv2.0 shall be provided to allow for secure storage and encryption of cryptographic keys in the controller.

Secure Boot

Secure Boot shall be implemented to ensure that the controller boots using only software that is trusted by the vendor and the user. When the controller starts, the controller firmware shall check the signature of each piece of boot software, including firmware drivers and the operating system, and only boot of the if the signatures are good.

Encrypted Firmware Updates

To support secure boot, firmware updates shall be signed and encrypted to ensure that the controller boot sequence cannot be compromised.

Software Development Lifecycle

The vendor shall use a secure software development lifecycle framework to cover the development of firmware and software. Security shall be built-in at all stages and not left until the testing stage. Security related activities shall include hiring and training of employees in secure development approaches, use of appropriate tools, consideration of security as a prime requirement and not an optional add-on, building and testing code with security in mind, use of third-party tools such as Wurldtech Achilles and other approaches as required.

Application Security

PLC Memory Protection

The process controller shall have four levels of security or password privilege levels to prevent

unauthorized changes to the contents of the process controller. These built-in privilege levels shall be set in the programming software or with the hand-held programmer and shall impose the following constraints:

Level Constraint

1. Read process controller data only (except passwords)
2. Write to any data memory
3. #2 and write to all configuration or logic in STOP mode
4. #3 and write to logic in STOP or RUN mode (on-line change) and password level access.

There shall be one password, one to four ASCII characters in length, for each privilege level in the PAC and the same password can be used for more than one level.

Any attempts to access or modify information in the process controller without the proper password privilege level shall be denied.

Subroutine Password

The process controller shall have a software OEM key that allows users to control access to each subroutine in the relay ladder program.

OEM Password

The process controller shall have a software OEM key that allows users to protect the resident program from unauthorized reads and writes.

Enhanced Security

An enhanced security feature shall be available to allow configuration of areas of Controller memory, symbolic variables and I/O variables to be marked as no access, read-only access, or read/write access and to allow strong passwords for the above.

Additional Cyber Security Products and Services

The vendor shall provide additional cyber security products and services including the following. The vendor shall be a world-recognized cyber security authority.

- Managed switches with cyber security capabilities.
- Firewall, intrusion protection system (IPS) and application-layer control appliances.
- Cyber security services including consultancy, security assessments, training and testing.

12 – Industrial IoT

General

The vendor shall support an open Industrial Internet of Things (IIoT) capability such as Emerson's Edge Controller. This shall include capabilities such as, python script interpretation, web server configuration, and SQL and/or time-series databases. The IIoT capabilities will not limit cloud vendors. The user shall not be restricted from managing the IIoT operating system directly. The IIoT capabilities should allow a user to create a local (edge) application with secure communication to the control system and not prohibit distributed edge and cloud applications. The IIoT capability should provide a firewall between the controller and IIoT operating system and between the IIoT operating system and upstream networks.

- Inner loop / outer loop
- The IIoT software should include capabilities for flow-based programming, modern web applications, Docker container runtime and multi-container management. At a minimum an application development specification and example application should be provided as a reference for users to develop on the IIoT software system.
- Standalone edge devices including….
- Physical specs…The IIoT software should be capable of running on both ARM and x86 CPU architectures. The IIoT software should be available pre-installed on ruggedized fan-less hardware capable of -20ºC to +65ºC without CPU throttling.