Specification
for a
Process Automation System

Contents

1 Introduction

1.1 Scope

This specification defines the minimum mandatory requirements for a Process Automation System and associated software and support services.

This specification excludes field instrumentation.

1.2 Project Objectives

To have a process automation system designed, manufactured and installed which exhibits high availability, reliability and safety yet is economical cost effective and allows the plant to operate at high efficiency at its continuous operation and maximum production during its design life. The system shall be robust at all levels and suited to the industrial application with low component failure rates.

To support plant wide control disciplines (continuous & discrete processes).

To have a system that seamlessly integrates with all other plant systems (power, auxiliaries, mechanical, civil, management, maintenance, etc.) that provides the most overall economical solution. The system shall provide standardized solutions for the digital integration of auxiliary systems such as motor control centers (MCC), drives, transmitters, package units, weighing systems, etc.

To fulfill scalability by using a single platform with scalable integrated or separated process safety including safety matrix for engineering & operation. To provide high controller performance and capacity with hot swappable-, standard, remote-, intrinsically safe and SIL2/3 safety inputs/outputs (I/O), optional redundancy on all levels including inputs and outputs and node redundancy.

The system shall have an integrated security concept covering the entire plant, companywide and external intranet/Internet/communications systems. The security concept shall be designed integrated and cover hardware, firmware and application systems for the process automation system lifecycle.

To have a process automation system with the highest level of compliance with international technical standards as listed in this document.

To have a system that can ensure project execution and implementation time are maintained, or improved on, due to its design and standardization. Through the availability of advanced engineering tools, process automation system engineering shall be configuration based rather than involving the development of specialist software code.

The system shall provide fast engineering and quick and reliable commissioning and integrated functions like batch, material management, route control, model predictive control. Availability of standardized, fully tested objects (function block + faceplate) for sensors, motors, valves in released libraries including specialist process graphic templates.

Asset management shall be supported with process performance monitoring of major equipment such as pumps, motors, heat exchanger, etc.

The system shall be designed for maximum operator ergonomic comfort with advanced alarm management technologies that support the reduction of alarms

and operator work load in a structured and safe way. Intuitive views shall provide situational awareness and better decision support.

The system shall help in constant and intensive utilization of the plant information for our production professionals, such as operators, production managers, maintenance and development engineers to achieve the best results due to they work towards the same goal.

To have a most modern, well supported and process automation system with an extensive existing established installed project reference list and proven design. The system shall have previously been installed for similar applications in a similar environment. The process automation system shall be from a reputable manufacturer with sufficient experience in the respective field of application. Solid support for the planned lifetime of the plant shall be demonstrated as well as for future expansions and upgrades.

The system shall significantly contribute to "operational excellence“, maximum throughput, availability and product quality, and at the same time minimize operating and maintenance costs, energy and raw material consumption, off-spec products, emissions and safety risks.

The Vendor shall have an open and published price list for hardware and system software and application packages that can be purchased from well supported network of distributors. It shall be possible that extensions, changes or modifications can be performed by a network of trained and certified third-party companies.

2 General

2.1 For All Applications

The process automation system shall be a Distributed Control System (DCS) for the purpose of controlling, monitoring, and managing of alarms and storage of process data including homogenous integration of programmable logic controllers and safety systems.

Hardware and software must be for the most part scalable to fulfill the wide-ranging requirements.

The system shall have multi-protocol interfacing capabilities in order to communicate with other systems and provide seamless horizontal and vertical integration.

The system should provide a client-server architecture.

The system must provide common hardware and development tools for various solutions.

The system shall be designed for DCS, safety and PLC (programmable logic controllers) applications. It must be capable of fulfilling high-speed requirements.

The system must offer integrated fail-safe features in runtime and engineering.

The system must support CiR (Configuration in Run).

The system must support fieldbus devices from any manufacturer without additional certification.

The vendor system must contain a high-performance Human Machine Interface (HMI) product which is owned, developed, manufactured and tested by the vendor.

The vendor system shall also support separation between the terminal and system bus if required.

The Vendor system must support the system redundancy and also media redundancy as a minimum requirement in fieldbus operation using PROFINET.

The controllers of the system must allow operation without a fan.

2.2 Combination of DCS, PLC, Batch and Safety System

The process automation system shall include features traditionally associated with both a programmable logic controller such as programming in ladder logic as well as a distributed control system (DCS) with remote I/O architectures and such as continuous and complex control, advanced operator interfaces, scalable redundancy on all levels.
These capabilities must seamlessly reside in one control system without the use of special gateways or interfaces.
In addition, the system shall provide seamless integration of continuous, batch and safety protection control, including common software tools.

2.3 Horizontal Integration

The system shall provide integration of process control tasks and upstream and downstream discrete control tasks such as raw material handling and packaging, permitting economical plant-wide integration of all operations in any manufacturing and process environment.

2.4 Vertical Integration

The system shall support vertical integration by utilizing uniform data communication structures to support complete integration from the Enterprise Resource Planning (ERP), Manufacturing Execution Systems (MES), control and field levels.

2.5 Open Systems

The system shall be based on well supported open / common commercial systems and technologies including Personnel Computer (PC) platforms with a Microsoft Windows operating system, Ethernet communications, TCP/IP, OPC for interconnectivity of multiple systems from different suppliers, field mountable control system, remote I/O subsystem, and bus-based serial communication with field devices over PROFIBUS-DP/PA, PROFINET, Foundation Fieldbus H1, HART, AS-I, and Modbus networks.

2.6 Decentralized Architecture

The system shall have a decentralized flat and client/server architecture allowing extensive scalability. The system shall be expandable and support up to 20 engineering workstations, 40 operator displays – where each station has access to the entire plant, eighteen redundant servers, and 128,000 process tags.

2.7 Scalability

The system shall be scalability without the provision of reserve capacities from hundreds to one hundred thousand of I/O's. A graded range of controllers shall be available providing scalable performance for different process requirements.

Controllers and I/O shall be interchangeable permitting changing of controllers to meet performance requirements.

The scalability of the system shall include software licensing as well as hardware configuration.

The functionality of the system shall be scalable permitting changing requirements to be met without change of controllers:

- Communication requirements (e.g. telecontrol)
- Operator interfacing (e.g. local display units)
- Integration of new data sets (e.g. asset management or power control systems)

2.8 Redundancy

The system shall offer optional redundancy at all levels to provide a high-level of fault tolerance. Operator stations, servers (including batch), historian, the terminal and system buses, controllers, field networks, and I/O modules or channels shall be capable of being made redundant as required. Redundancy shall be achieved with event-driven synchronization which has fast and bumpless changeover to the redundant central processing unit (CPU) in the event of a fault.

A single failure anywhere in the system shall not result in the loss of regulatory control to more control loops than those associated with a single process input/output card. Failure of any single device shall not affect the ability of the system to communicate with other devices in the system. Switchover shall not disrupt any system functions.

Redundant equipment and software shall be continuously monitored for errors. All modules shall be diagnosed on-line. Errors shall be alarmed with an error message identifying the failed module.

To maximize data availability and integrity, the operator interface shall provide the ability for configuration of system redundancy. This shall in no way limit or restrict the use of the client/server configuration and/or architecture.

Clients shall automatically failover to the backup or redundant server. This operation shall not require any application reprogramming or reconfiguration.

System redundancy shall be configurable on a '*server-by-server'* basis up to a profile of eighteen redundant servers.

Client stations shall support the designation of different primary servers allowing the network loading to be distributed and to ensure that in the event of a failure not all clients will experience a switchover.

Once a failed server becomes available, the active server shall check and restore missing data to the failed server. The data recovery operation shall occur in the background, and shall not affect the operation of the on-line server.

The redundancy at each level (field I/O, controller, communication, servers, and operator) shall be configured flexibly according to requirements. Physical separation of redundant pairs shall be possible.

Redundant fieldbus architecture allows multiple errors without causing interruption. A ring-shaped fieldbus should be used to increase availability.

I/O redundancy shall not be dependent on CPU redundancy.

It must be possible to create two process variables (tags) under the same name and to use integrated redundancy functions (without new programming). It must also be possible to connect redundant process variables (tags) at various I/O racks.

2.9 Availability

The system shall provide high equipment reliability. The high reliability shall be demonstrable based on field proven designs under similar environmental conditions. The Meant Time Between Failure (MTBF) of equipment shall be available.

The reliability shall be demonstrable for:

- Hardware, firmware and software components (controllers, servers, etc.)
- Communications components
- I/O
- Peripherals (operator systems, field panels)
- Auxiliary components (system clocks, etc.)

To reduce Abnormal Shutdown Time (AST) maintenance shall be based upon simple replacement of the faulty equipment identified as faulty by the system itself. The system shall have demonstrable low Mean Time Repair (equal to AST). Comprehensive self-diagnostic facilities shall support identification of faulty equipment with simple alarms to operators.

The system shall be qualified with certification to meet relevant safety complying with the applicable national and international standards such as requirements:

- IEC 61508 (up to SIL 3) functional safety for industry
- IEC 61511 / ANSI / ISA-84 for process industry
- IEC 62061 / IEC 60204-1 / ISO 13849-1 for machinery industry

The design of process control systems shall be such that the failure of any component of the system shall have minimal effect on the process. The components shall have proven high integrity and be rugged and physically compact.

The process control system shall be designed for 99.99% (to 99.9999) availability by the inclusion of built in redundancy for both hardware and software. This shall include redundant control processors, redundant I/O cards, redundant data highways and redundant power supplies with automatic changeover to the hot standby unit on detection of a fault or failure of the operating unit. Each controller in a redundant configuration shall communicate with both data highways.

Availability shall be defined as:

$$\% \text{ Availability} = \frac{100 \times MTBF}{MTBF + MTTR} \quad \text{or} \quad \frac{100 \times (OPT - AST)}{OPT}$$

Where:

OPT = Operating Period Time (h) (includes shutdown time)

AST = Abnormal Shutdown Time (h)

2.10 Online Changes

The system shall support the ability to make the following changes online without interrupting operations:

- Changing the parameters of an I/O channel
- Adding or removing an I/O Module
- Adding or removing a rack of I/O
- Adding or removing a PROFIBUS DP slave
- Adding or removing a PROFIBUS PA field device
- Adding new connections to Industrial Ethernet networks
- Modifying the range of an analog point
- Modifying a process graphic
- Adding a new tag to the archive database adding a new control loop to the configuration

2.11 Licensing

Software licenses for engineering workstations and for operator interface consoles shall be independent of the type and mixture of I/O used (analog vs. discrete, input vs. output).

The software licenses (both runtime and engineering) shall be portable allowing the user to transfer licenses from one PC to another without requiring intervention from the vendor.

License Model

The vendor must offer a clearly delineated licensing model.

The vendor must offer a licensing procedure that is based on the number of process objects (PO) for operator station (OS) and controller in the application.

The engineering system shall show the licenses in use and reserve capacity.

2.12 Use of Standard Products

The system shall be composed of manufacturer's standard hardware, systems software, and firmware that can be configured to meet the stated requirements for which the manufacturer is able to provide long term support and guarantee quality. The vendor's standard system operating software shall not be modified to meet any of the user's requirements.

Application software shall be implemented using the standard process automation system without requiring modification to its system software or operating systems.

The original manufacturer of each type of component in the offer shall be listed.

2.13 Spare Capacity and Expansion

Each system shall be supplied with XX% spare capacity for each I/O type in the base system. The base system is defined as the quantity of hardware needed to meet the project requirements.

Communication networks shall be designed to allow for system growth of at least XX% based on the number of unused node addresses. System expansion shall be achievable without shutting down the controllers not directly involved with the expansion.

System Runtime and Engineering Software shall be capable of being expanded by the purchase of additional licensing units.

2.14 Special Applications

PC based controllers shall be available for special applications (e.g. for package units, laboratory automation, widely distributed automation tasks). The controller shall provide a Windows Operating System with Real Time Extensions (RTX). It shall be possible to network and integrate the many controllers for larger applications.

The controller shall have a construction design as per process automation system without fans or rotating media meeting the same design temperatures and vibration standards suitable for 24-hour continuous operation in an industrial environment. The controller shall make use of the standard process automation system I/O modules.

The controller shall integrate with the process automation system having Ethernet PROFIBUS and PROFINET interfaces as well as standard USB interfaces for local peripheral connection.

The controller shall be suited for both autonomous stand-alone operation (e.g. tank farms, water industry applications which have widely distributed automation tasks) or fully integrated in to the process automation system (e.g. typical for package units).

3 Environmental Conditions

3.1 Indoor Installations

Equipment installed in buildings shall be designed to operate in the following environmental conditions:

- Temperature range: 0 °C to +50 °C[1].
- Relative humidity: 5% to 95% RH

3.2 Outdoor Environment

Equipment installed outside shall be designed to operate in the following environmental conditions:

- Temperature range: -40 °C to +70 °C[2] (no direct sunlight)
- Relative humidity: 5% to 95% RH.

3.3 Component Design Environment

Components installed in panels shall be designed to operate in the following conditions:

CPUs

- Temperature range: 0 °C to 70 °C[3]
- Conformal Coating: industrial standards (ISA-S71.04 severity level G1; G2; G3)
- Relative humidity: 0% to 95% (without condensation)

Power supply unit (PSU)

- Temperature range: 0 °C to 70 °C[4]
- Conformal Coating: industrial standards (ISA-S71.04 severity level G1; G2; G3)
- Relative humidity: 0% to 95% (without condensation)

Peripheral devices

- Temperature range: -40 °C to 70 °C[5]
- Conformal Coating: industrial standards (ISA-S71.04 severity level G1; G2; G3)
- Relative humidity: 5% to 95% (without condensation)

Networking devices

[1] Adjust to requirements
[2] Adjust to requirements
[3] Adjust to requirements
[4] Adjust to requirements
[5] Adjust to requirements

- Temperature range: -40 °C to 70 °C[6]
- Relative humidity: 0% to 95% (without condensation)

IPC severs / clients

- Temperature range: +5°C to 50 °C[7] Tested according to IEC 60068-2-2, IEC 60068-2-1, IEC 60068-2-14
- Relative humidity: 5% to 95% (without condensation)

The component design shall allow for configuration of control equipment without fans or air-conditioning.

3.4 Hazardous area requirements

Equipment located in hazardous areas shall be designed and installed in accordance with ATEX 137 Explosive Atmosphere Directive (99/92/EC) and the National Electric Code NFPA 70 Article 500/505.

Electrical and control rooms and generally process areas are classified as safe areas unless a specific hazardous area classification is assigned.

3.5 Storage Environment

It shall be possible to store the equipment before installation for up to 6 months in under the following conditions:

- The equipment shall be packed in a moisture proof container
- Storage temperature: -40 to 70 °C (no direct sunlight)
- Relative humidity (outside the moisture proof container): 5% to 95%

3.6 Equipment Environmental Protection[8]

Protection of electrical enclosures and equipment against dust and water ingression shall be according to IEC 60529:

- Control rooms IP20
- Process areas IP54
- Outdoor (naturally ventilated and wash down areas) IP55

[6] Adjust to requirements

[7] Adjust to requirements

[8] Amend according to requirements

4 Electrical Requirements

4.1 System Power

The electrical power supply shall be:

- Voltage: 100/110/120/230/240 VAC or 5/24/48/60 VDC
- Frequency 50/60 Hz

4.2 Electromagnetic Compatibility

Equipment shall meet all electromagnetic compatibility requirements of the IEC 61000-4-2, 61000-4-3, and 61000-4-4 standards.

4.3 Wiring and Cabling

PROFIBUS, Industrial Ethernet, and other communication cables shall maintain a minimum separation of 75 mm from any AC power cables. Fiber optic cables are excluded from this requirement.

Vendor installed cables shall be designed and installed in such a way as to allow cable disconnection in order to service the equipment. Cables shall not interfere with circuit board removal.

Connectors and modules shall be mechanically designed that short circuits or incorrect polarity is prevented on insertion or when connections are made.

4.4 Cabinet and Workstation Grounding

AC Safety ground and instrumentation circuit ground shall conform to the IEC 61131-2 (or NEC, Article 250).

4.5 Circuit Boards

It shall not be necessary to remove power or field wiring to replace a control or input/output module.

5 Controller

5.1 Multipurpose Controller

The controller shall be a multipurpose controller capable of executing fast PLC-type programs (discrete) and DCS-style applications (regulatory) allowing process and machinery control to be integrated in one device. Extremely short instruction processing times down to 10 ms., required for programmable logic control, and slower processing times required for process control, shall both be available. A minimum of 9 independent application cycle rates should be available for optimizing the execution time of the application program.

The controller shall support all connections and requirements / standards mentioned in chapter 7 "Fieldbus". In relation to PROFINET standards, the controller shall support media redundancy (MRP).

5.2 Large Capacity Controller

The controller shall be capable of executing a minimum of 1000 standard Proportional Integral Derivative (PID) control loops with a 500 ms. sampling rate to reduce the need for partitioning of the user application program.

A controller of the upper performance class must be offered with the following performance specifications:

Instruction processing execution time: 18ns

Memory: 30 MB

It shall be possible to configure controllers with I/O from 100 up to 4000 points.

A cold start shall not require the use of an engineering workstation.

The process automation system shall support extensive application program documentation and commenting without any detrimental effect on CPU performance or controller memory.

The controller shall have PROFIBUS connections and at least two PROFINET connections. The operation of 500 PROFINET devices on one controller must be guaranteed.

5.3 Controller Redundancy

For high reliability applications, redundant controllers, -power supplies, -Ethernet -connections, -racks, -PROFIBUS and –PROFINET networks shall be available.

Regarding the PROFINET standard, the redundant controller must support system redundancy S2 and redundant PROFINET configuration R1.

Redundant controllers must support changeability during operation (CiR).

Firmware updates shall be possible for redundant systems during ongoing operation.

Physical Separation of Redundant Controllers

When required it shall be possible to physically locate redundant controllers in separate panels/rooms/buildings to mitigate any risk potential from common cause failures (e.g. fire). A separation distance of >1,000 m shall be possible.

Switchover Time with Redundant Systems

In a redundant system, controllers shall operate with a “hot backup” where both CPUs execute the identical step of the user program in parallel. When a CPU error is detected, a bumpless switchover shall be initiated between the controllers. The complete switchover shall be completed in approximately 10 ms or less including all I/Os and including no loss of alarms or messages.

Connected redundant I/O components must switchover within 20 ms if a fault occurs.

5.4 Power Components

Power Supply

There shall be a choice of a 24 VDC or 60/80/110/120/230 VAC 50/60 Hz power supply.

Battery Backup

Controller configuration memory shall have a battery backup so that the controller maintains its configuration and state information in the event of an extended power outage. The program execution shall resume in a predetermined safe condition upon power restoration.

5.5 Choice of Configuration Languages

Configuration languages shall be offered that are traditionally associated with both a DCS and a PLC programming environment. The system shall support graphical and textual programming languages as per IEC 61131-3:

- Instruction List (IL)
- Structured Text (ST)
- Function Block Diagrams (FBD)
- Ladder diagram (LD) Language
- Sequential function chart (SFC)

In additional the system shall support the industry language Continuous Function Charts (CFC) and the configuration of cause and effects as per ISO 10418 safety matrix for safety applications.

5.6 Closed-loop-control

Standard software algorithms shall be available to perform regulatory control functions, and these shall have easily configurable parameters.

5.7 Control Modes

It shall be possible to put any individual control loop in a manual; automatic, or cascade mode. In cascade, it shall be possible to configure remote setpoints from other regulatory controllers or from other control blocks.

There shall be bumpless, balanceless transfer between all control modes, and windup protection shall be provided.

Control blocks shall be able to perform automatic mode switching based on external or internal logic inputs.

5.8 Calculations

Algorithm calculations shall be performed in floating-point engineering units or other such equivalent methods that do not require scaling.

Input Functions

The following input functions shall be supplied as standard configurable items:

- Square root extraction, for flow measurement
- Linearization of type B, E, N, J, K, L, R, S, T, and U thermocouples
- Linearization of resistance temperature detectors (RTDs)
- Digital input pulse totalization
- Pulse input to frequency conversion

Computational Functions

The following computational functions shall be supplied as standard configurable items or simple algebraic instructions.

- Addition / subtraction
- Ramp generator
- Lead lag
- Integrator / Accumulator
- Dead time
- High/low select
- Multiplication / Division
- Time averaging
- Signal selection switch
- Exponential polynomial

- Logarithms
- Square root
- Absolute value
- Closing delay
- Min/Max selection
- Smoothing function
- Noise generator
- Signal smoothing / low pass filter
- Alarm delay

Continuous Control Functions

The following control functions shall be configurable items:

- PID
- Auto/manual with bias control
- Ratio control
- Step Controller
- Split Range Controller
- Cascade Control
- Override control
- PID with feed-forward
- PID with Smith predictor
- PID with safety logic and control loop monitoring
- PID with operating point-oriented parameter adaption
- Model predictive control
- Adaptive tuning (optional)
- Fuzzy logic control (optional)
- Multivariable Control (optional)

Control Loop Execution Frequency (Scan Rate)

It shall be possible to independently select the execution frequency of each device control strategy in the controller. Controller shall process tasks and scan I/O as fast as 100 times per second (10 ms).

Control Loop Output Functions

The following output functions shall be supplied as standard configurable items and shall be the same regardless of execution in the system controller:

- Linear
- Linear with clamping (high and low restricted)
- Non-linear characterization

Setpoint Clamps

Upper and lower clamps on all setpoints shall be configurable.

5.9 Discrete Control

The following discrete control functions shall be supplied as standard configurable items:

- Logic functions -- and, or, not, nand, nor, xor
- Change of state detect
- Set/reset flip-flops
- Timers and counters
- Comparison elements -- greater than, less than, equal to, not equal to
- Multiplexer (selects one of up to 16 signals)
- Positive, negative, and bi-directional edge trigger

The vendor system must be able to support wide-ranging technological modules (controllers, positioners, counters etc.).

5.10 Sequential Control

Sequential Function Charts (SFC) shall be available. SFC is a structured, IEC 61131-3 compliant, high-level control programming language.

The SFC shall include the following features:

- +It shall provide the necessary facilities for real-time control of sequential processes.
- It shall have access to process control and other database information.
- It shall be possible to modify the program logic while other sequences are active.
- It shall support execution of the chart in Manual or Automatic Mode
- It shall be possible to configure multiple states within a single SFC container. This allows for effective coordination of sequences which have more than one mode (e.g. heating and cooling) or that contain safe-state logic (e.g. aborting or holding logic)
- The ability to create master SFC elements which can be copied and used throughout the configuration just like a function block. Changes to a single

instance of the SFC will result in automatic updates to all other instances in the configuration.

- The ability to automatically create displays for visualization and control of the SFC directly from the controller configuration.
- The SFC editor shall include a test/debug mode which does not write to the outputs
- Manual adaptation following name changes in charts and their references should not be necessary.
- Sequential charts in OS: It must be possible to monitor the sequencer of the vendor system and operators must be able to intervene if disturbances occur in the process.
- It must be possible to perform actions in step transitions.
- In the case of several overlaid SFCs that use the same underlaid SFCs, the assignment and administration must take place on the system side.

Sequential Functions

The following sequential functions shall be supplied as standard capabilities:

- Hold sequence - Manual or preset time
- Recycle to prior step
- Skip one or more steps
- Automatic restart at beginning upon completion (cyclic operation)
- Configuration of maximum or minimum execution times for steps and transitions
- Ability to configure an optional operator confirmation for each individual transition condition

Step Control Modes

The way in which chart progresses from a transition condition to the next step can be controlled according to the following modes:

- Transition – Control is governed solely by satisfying the transition condition
- Confirmation – Control is governed solely by operator confirmation
- Transition and Confirmation – Both the transition condition must be satisfied and the operator confirmation must be entered before the sequence will proceed
- Transition or Confirmation – Either the transition condition is satisfied or the operator confirmation is entered to allow the sequence to proceed

Phases of a Step

Each step of a chart shall support the following standard phases of step execution:

- Initialization – For first-time execution of actions
- Execution – For continuous execution of actions until transition condition is met
- Termination – For post-processing to allow an action to be executed once after the transition condition has been met

Supported Operating States

The following 16 SFC operating states (per the S88 standard) shall be supported natively by the system:

- Ready
- Starting
- Active
- Completing
- Error (Completing)
- Completed
- Holding
- Held
- Resuming
- Error
- Held (error)
- Resuming (error)
- Aborting
- Aborted
- Stopping
- Stopped

5.11 Supervisory Control

The process automation system supervisory functions shall be fully integrated with the controller functions. The supervisory functions will include the ability to make setpoint adjustments to selected loops.

It shall be possible for supervisory control applications to be scheduled, run on demand, or triggered by events.

The supervisory system shall have access to the complete database, with privileges to change items such as controller mode and setpoint.

5.12 Auto Tuning

An integrated PID auto tuning facility shall be available from the Engineering Station:

- Applicable to processes with slow and fast dynamics
- Used with self-regulating and integrating processes
- Immune to noise and process load disturbances
- Can be used for standard and custom libraries
- Can be accessed directly from the Engineering Station

The PID auto tuning facility shall employ an easy-to-use graphical interface with a setup “wizard“ to assist engineers and technicians who are unfamiliar with the tool.

5.13 Fault Handling

Invalid value status shall be generated for inputs and calculated variables.

A value shall be declared invalid if any of the following conditions are true:

- If a value is out of range
- If a value cannot be measured or calculated
- If a value is declared invalid by an application program
- If a value is declared invalid by the source instrument

Invalid value status (data quality) shall be propagated through control schemes, and be available at the HMI.

It shall be possible to inhibit the detection and propagation of an invalid value status. This selection shall be available on a per tag basis.

It shall be possible for an invalid value status to be used as a logical input to initiate control algorithm changes.

When a control algorithm's input is declared invalid, it shall be possible to configure the output to fail as follows:

- Hold last good value
- Zero output signal
- User defined output value

In the event of communications subsystem failure, regulatory control algorithms shall continue operating with the last valid information.

.

5.14 Variable Scan Rates of Control Functions

The control execution rates for analog functions and discrete functions shall be individually configurable.

The minimum program processing cycle for discrete and analog control functions shall be 10 ms.

5.15 Cabinets

Control cabinets shall conform to EU CE standards for electromagnetic compatibility (EMC) according to IEC 61000, and ensure protection against unauthorized access, mechanical influences, contamination, and other environmental influences.

The standard cabinet shall conform to IP20 and up to IP55 shall be available according to environmental conditions.

5.16 Controller Communication over System Bus

The system bus used for communication between controllers and up to the HMI servers shall be capable of running at 100 Mbps/1 Gbps data rate.

Use of fiber optic cables shall be supported, allowing noise free communication between control and operator stations separated by large distances as required by many processing facilities.

ITP (Industrial Twisted Pair) cables are to be used for distances up to 100 m.

The length of the system bus shall be expandable to 150 Km.

The system bus shall support from two to 1024 stations.

For maximum availability, the system bus shall support configuration in a double redundant ring architecture, using either fiber or copper media.

5.17 Reserve CPU Capacity

To reserve CPU capacity for future growth and ensure rapid software response to process upsets, CPU execution of the configured software application shall not exceed XX% CPU loading during the course of normal process monitoring and control.

6 Inputs and Outputs

6.1 General Inputs and Outputs

Common mode rejection ratios of 60 dB or greater from DC to 60 Hz and normal mode rejection ratio of 30 dB or greater at 60 Hz are required.

The system must provide the electrical isolation between the channels in a module-specific manner.

Analog input and output modules shall provide pass through capability to exchange non-control data, PROFIBUS, PROFINET and HART, with asset management applications, utilizing the infrastructure of the system.

The following configurable fail-safe options shall be available for output modules:

- Drive to predetermined analog output, or de-energize for a digital output
- Maintain the last good output value for an analog, or hold for a digital output.

The fail-safe actions listed above shall be taken upon a processor halt, or power supply failure, or a communication failure between the controller and the I/O module, if so configured.

It shall be possible to change modules in remote I/O racks while the rack is powered up w/o affecting communication to the other modules in the rack.

6.2 Support for Remote I/O Architectures

Remote I/O Capability shall be provided native to the system to minimize wiring costs and to eliminate the need for costly “home run” wiring – The system shall support the following remote I/O families:

- Intrinsically Safe (EEx-i) - For installation directly in Hazardous Locations (per NEC Class 1 Div 2, Zone 1 / Zone 2)
- Support of Fail-safe Applications
- Integration of HART field devices
- With Integrated Terminal Blocks
- With special-purpose modules such as Motor Starters and Weigh scales
- With various levels of diagnostics and resolution (number of bits)

The PROFINET station family must have the following functions:

- System redundancy S2
- Media redundancy MRP
- Changeability during operation

To achieve flexibility in the placement of equipment, the vendor’s system shall support remote I/O installation whereby conventional I/O modules can be located large distances away (9.6 km with copper cable or longer distance when fiber-optics are used) from their associated controller.

6.3 Redundancy

The system shall support the use of I/O redundancy whereby a single sensor or actuator is connected to two separate I/O modules.

A redundant controller can utilize a mixture of redundant I/O and non-redundant I/O within the same system.

To minimize the potential for common cause failures, redundant I/O modules must be able to be located in physically separate racks. It is not permissible to share a common backplane.

For minimizing the errors in the PROFINET environment a red. Power supply, a red. PROFINET connector (S2 or R1) and a red. I / O module are required.

The system should offer optimal integration of redundant Remote I/O racks (RIOs), redundant I/Os and fieldbus (PROFIBUS PA and DP and PROFINET), with both redundant and non-redundant models.

It must be possible to create two process tags (process variables) with the same process name and apply integrated redundancy functions without additional programming work.

6.4 Analog Inputs

The system shall be capable of supporting the following types of analog process input signals:

- 4-20 mA DC, 0-20 mA DC, and ±20 mA DC, isolated and non-isolated inputs
- 1-5 V DC, ±10 V DC, ±5 V DC and 0-10 V DC isolated and non-isolated inputs
- Type B, E, J, K, L, R, S, T and U thermocouples
- Platinum resistance temperature detector (RTD) – PT100, PT500, PT1000, Ni100, Ni1000, Cu10 - per IEC 60751
- High-speed Pulse input – 1, 10, 20, 100, 250, 500 kHz, @ 24 V

Temperature linearization and thermocouple cold junction compensation shall be provided.

Normal resolution shall be a minimum of 12-bits; special modules with 16-bit resolution shall be available.

Typical analog input modules shall operate at 25 °C with a basic error of no more than ±0.25% of input range

6.5 Digital Inputs

The system shall be capable of supporting the following digital input types:

- 24 VDC (capable of being time stamped to 1 ms accuracy)
- 125 VDC
- 48-120 V DC
- 24-48 VAC/DC, 50/60 Hz
- 120 VAC, 50/60 Hz
- 230 VAC, 50/60 Hz

6.6 Analog Outputs

The system shall support output types of 0-20 mA, 4-20 mA, ±20 mA, ±10 V DC, 0-10 V DC, and 1-5 V DC.

Analog output modules shall operate with an error limit less than the following:

- Voltage ±0.2% of output
- Current ±0.3% of output

6.7 Digital Outputs

The following solid state output ratings shall be available:

- 24 V DC
- 48-120 V DC
- 20-125 V DC
- 120 V AC, 50/60 Hz
- 230 V AC, 50/60 Hz

Relay or solid-state output contacts that are free of voltage and ground shall be available.

Relay outputs with 24 VDC to 120 VDC, 48 VAC to 230 VAC, 5A rating shall be available.

Digital output module with actuator shutoff via low signal or high signal must be available.

6.8 Marshalled Termination Assemblies

To reduce installation costs and startup time, the system shall offer a standard set of Marshalled Termination Assemblies (MTA) as a means of providing fast and easy connection to the field level while preventing wiring faults. These termination assemblies shall provide an individual protection of each channels and also individual blown-fuse indication and redundant power connections. A common MTA shall support connection to a redundant or non-redundant I/O configuration.

The PROFINET field devices must have the following characteristics for a fast and simple (avoiding wiring errors) connection to the field level via PROFINET:

- Highest availability at PROFINET via system redundancy S2 or redundant PROFINET configuration R1
- Integrated IO redundancy (without MTA)
- Modular exchange during operation
- Media Redundancy (MRP)

6.9 I/O Bus Properties

The I/O bus must have the following properties:

- Avoids unplanned plant down-time with increased availability
- Automatic bus termination
- Detailed diagnostic options
- Changes to the configuration can be performed online. The also takes into account repairs and add-ons including changes on the cable bus.

6.10 I/O Bus Redundancy

It must be possible to configure a redundant I/O bus.

The vendor shall provide coupler redundancy.

The vendor must provide a redundant ring structure of the I/O busses.

It must be possible to perform value acquisition from field devices as fail-safe (1oo2) and fault-tolerant (2oo3), the vendor must ensure this with his bus architecture.

6.11 I/O, instrumentation and couplers

The I/O Interfaces and couplers must be integrated in the alarm system of the control system.

The I/O Interfaces and couplers should optionally offer recording of events (SOE Sequence of Events).

The I/O interfaces should support high channel density (i.e. >320 discrete or >80 analog I/O).

The I/O interfaces / couplers shall support HART sensors.

The scan rate for all channels shall not be longer than 120 ms.

A 1 ms time stamp for DI must be available (SOE= Sequence of Event Recording)

The system shall be capable of closed loop sampling rates of 10 ms.

6.12 Open I/O Communication

Open standards should be used to communicate between a controller and its I/O modules to facilitate connectivity of third-party I/O with the same level of system support (diagnostics and engineering ease of use) as those offered by the vendor. It shall not be acceptable to utilize proprietary communication between the I/O and the controller.

Communication between controller and I/O should be in accordance with IEC 61158 PROFINET.

6.13 AS-Interface I/O

The system shall support AS-Interface inputs and outputs for discrete devices such as switches and solenoids. The AS-interface shall be a link module on PROFIBUS-DP, communicating with the devices over the AS-Interface serial cable.

6.14 EIB Instabus I/O

The system shall support EIB Instabus inputs and outputs, as used in building automation systems, allowing the building control system and the plant control system to be combined into one. The EIB interface shall be a link module on PROFIBUS communicating with the devices over the EIB serial cable.

6.15 HART I/O

The system shall support HART inputs and outputs. The HART interface shall be a module on PROFIBUS, or the HART devices can be connected to conventional analog input/output modules. All components shall have plug and play capability. The engineering system shall be able to read all variables provided by the field device without the need for any additional wiring.

7 Fieldbus

7.1 General Requirements

The system shall be able to read all variables provided by the field device without the need for any additional wiring.

Diagnostic information shall be available from the field devices, including device faults, configuration faults, operating mode, and maintenance requests.

Compatibility with third-party Devices

The system shall support all field devices certified by the appropriate standards body for that fieldbus type and shall not require additional approvals by the vendor of the host system.

7.2 Fieldbus PROFINET

The automation system must support PROFINET as part of IEC 61158 and IEC 61784-2 standards.

The system must ensure the connection of PA devices and DP devices / segments in the PROFINET fieldbus.

Maximum Communication Bandwidth

PROFINET must support a transmission bandwidth of 100 Mbit / s in full duplex mode.

Data per Device

PROFINET must allow up to 1440 bytes of user data per device.

Network architecture

The network architecture must be individually adaptable to the system via ring, tree and star topologies with one or more IO controllers.

Number of PROFINET devices per controller

PROFINET interfaces of the controller must support the connection of up to 500 PROFINET devices.

Maximum Segment Length

The maximum segment length between two PROFINET devices must be up to 100 m for copper cables and several kms for fiber optic cables.

The following functionalities must be supported by the system:

System redundancy S2, redundant PROFINET configuration R1 and Changeability during operation.

Support of switches

The System must have MRP-capable switches, which allow the connection of devices with system redundancy S2 to redundant PROFINET networks R1, thereby the network separation of the R1 networks remaining unchanged.

Support of Industrial Wireless LAN (IWLAN)

The system must ensure the connection of up to 8 PN-devices behind WLAN-Clients with S2 and R1 redundancy.

7.3 Fieldbus PROFIBUS DP

Fieldbus segments

The fieldbus segments shall support up to a maximum of 125 slave nodes (devices) such as analyzers, variable frequency drives and motor protection devices where each device is capable of bringing in multiple process measurements.

Maximum Communication Bandwidth

To minimize the number of segments (networks) required the PROFIBUS DP implementation shall support communication rates of up to 12 MB/sec.

Interfacing to Redundant Media

The system shall support connection of non-redundant slaves to a redundant PROFIBUS. The system shall support the combination of redundant and non-redundant PROFIBUS segments.

Maximum Cable Length

The system's serial multi-drop PROFIBUS DP network shall employ a two-wire cable, and support a maximum cable length of up to 9.6 Km / 6 miles. With the use of optional fiber optic cables there shall be no practical limitation in maximum cable length.

Number of Segments per Master

The system shall support up to 8 PROFIBUS DP Segments per PROFIBUS Master System

Number of PROFIBUS Masters per Controller

It must be possible to connect to a controller up to 4 PROFIBUS DP lines through internal interfaces in the CPU, and up to 10 PROFIBUS DP lines through additional communications processors. On a PROFIBUS DP line it is possible to operate up to 125 devices, and on a bus segment up to 31 devices with PROFIBUS DP interface (32 stations).

Online Device (Slave) Addition

The system shall support online addition of PROFIBUS Slave Devices to a PROFIBUS DP network, even in systems with non-redundant controllers.

Direct Support for Control of Motors and Drives

The system shall support direct support control of intelligent motor control center devices via PROFIBUS DP without requiring the use of gateways or interposing PLCs for control of:

- Motors
- Valves
- Variable speed drives (VSD)
- Soft starters

7.4 Process Fieldbus PROFIBUS PA/Foundation Fieldbus H1

Communication rates with process field devices connected to the PROFIBUS PA/ Foundation Fieldbus (FF) H1 shall be 31.25 Kbps. An H1 ring topology should be available such that a disconnect or cut in the ring will still allow communications to all field devices.

Interoperability

The system shall support the use of devices from multiple manufacturers on the same fieldbus.

Interchangeability

The system shall support the ability for a field device from a given manufacturer to be replaced by one of the same type (e.g. temperature measurement instrument) from a different manufacturer without loss of functionality. The configuration software shall support these features.

Minimize Wiring Costs

To minimize wiring costs it should not be necessary to run individual cables for each PROFIBUS PA/FF H1 segment from the field all the way back to the vicinity of the controller.

Number of Devices per PROFIBUS PA/ FF H1 Segment

The PROFIBUS PA/FF H1 fieldbus segment shall support up to 31 devices in a general purpose area and up to 9 devices in an intrinsically safe (EEx-i) area (assuming an average 12 mA current draw per device).

Minimizing the number of Physical Devices

To minimize the potential points of failure in the system, no separate physical device connection should be required to provide power to field devices.

Integrated Bus Terminator

The system's PROFIBUS PA/FF H1 interface shall include a power conditioner and an integrated bus terminator to reduce the number of points of failure and to reduce the labor cost to wire the segment.

Support for Intrinsically Safe Areas (EEx-i)

The system shall support placement of PROFIBUS PA/FF H1 field devices in intrinsically safe areas (up to Class 1 Div 1 / ZONE 1).

Integrated Barrier for Intrinsically Safe Areas

The Vendor's gateway to the intrinsically-safe PROFIBUS PA/FF H1 fieldbus segment shall include built-in intrinsically-safe barriers to connect these types of devices.

Foundation Fieldbus Integration

The vendor shall be able to integrate field devices connected via FF into the control system architecture.

The System shall have an interface that allows the user to connect FF devices to the system. The following functions should be supported:

- Cyclic and acyclic data exchange
- Diagnostics
- Integration in the systems maintenance station
- "Control In The Field"

7.5 Redundant & Fault Tolerant Process Fieldbus

To make it practical for users with mission critical applications, the system shall support the creation of optional redundant / fault tolerant architectures at PROFIBUS PA / FF H1 level

High Availability through fault tolerance

To allow mission critical process instrumentation to keep running in the event of communication faults, the system shall be able to sustain the following types of faults without interruption:

- Breakdown of the fieldbus Coupler
- Short circuit or wire break on the fieldbus backbone
- Short circuit or wire break on a fieldbus spur segment
- Loss of / Missing terminator

Online Configurability

The system shall support the making of online configuration changes such as repairs, extensions and modifications to trunk lines.

7.6 Fieldbus Distributor

Fieldbus distributor for PROFIBUS DP

To decrease the costs of installation and maintenance, the system shall support the use of field distribution boxes for connection and termination of multiple smart field devices. The field distribution boxes shall provide the following capabilities:

- Automatic monitoring of trunk line
- Support connection of at least 8 instruments
- Automatic bus termination
- IP65 case, PG connectors
- Short-circuit proof spurs
- Temp. range: -25° to 60° C
- Usage within zone 2 (Class 1 Div.2)
- Diagnosis through LEDs

Fieldbus distributor for PROIBUS PA field devices via PROFINET

The system must provide appropriate connection modules for the connection of PA field devices. These connection modules must have the following characteristics:

- Easy integration into the process control system
- Automatic initialization
- Automatic monitoring of the bus
- Connection of at least 8 PA devices
- Automatic bus termination
- IP66 case
- Temp. range: -40° to 70° C
- Usage within zone 2 (Class 1 Div.2)
- Diagnosis through LEDs

In addition, the bus distributor should have configurable channels (digital inputs / outputs) for easier integration of sensors or actuators

General requirements for field bus distributors

The fieldbus distributors shall provide protection against fieldbus short circuits and wire breaks so that distributors/fieldbus devices remain unaffected.

Installation, extension, removal or exchange of fieldbus distributors/devices shall be possible without affecting existing connected devices including any affects caused by incorrect termination and/or chattering (multiple connect/disconnect) during (de)installation. Complete physical layer separation of trunk and spur segments shall be provide.

The fieldbus distributors shall have integrated diagnostics.

The distributors shall be available in both industrialized and EEx (ia) version and suitable for Zone1/2 certified.

8 Communications and Networking

The system shall utilize Industrial Ethernet on the System Bus for communication between controllers and HMI servers or single stations.

The system shall support the use of standard commercial, off-the-shelf networking components for the terminal bus to communicate between servers and clients.

The system shall support the use of Fiber Optic and Copper (Twisted Pair) media.

The system shall support communication at 10 Mbps and 100 Mbps on the system bus and up to 1000Mbps on the terminal bus network.

A project-spanning network view must be available.

Intelligent field devices (PROFIBUS DP, PA, HART, FF, PROFINET) shall be accessible via an integrated configuration tool.

The system shall be able to control and diagnose intelligent drives via the fieldbus

The system shall support WLAN wireless networks.

The following maximum network sizes shall be supported: Electrical – up to 1.5 km, Fiber Optic – up to 150 km, WAN – worldwide (incl. Web-client).

The vendor system should offer networking options and support hybrid applications and linking of package units.

8.1 Supported Network Architectures

The system must support the ring and ring redundancy topology when setting up the system bus, as well as the linear-, tree-, and star- network topologies.

The System must support the ring and ring redundancy topology when setting up the Terminal bus, as well as the linear-, tree-, and star- network topologies.

The system must support the following network topologies when setting up the fieldbus: Linear, Tree, Ring, Star and Redundant.

For the ring topology, the system must ensure that all participants in the network remain accessible when the ring structure is interrupted.

For the highest availability requirements, the system bus and / or terminal bus must be designed for redundant rings.

8.2 Industrialized Smart Switches

Optional smart switches shall be available for use with the system that are designed for use in industrial environments. These switches shall have the following characteristics:

- Support for Fiber Optic or copper media
- Built-in digital inputs that can be wired into the system to alert users of networking faults
- Signaling contacts to alert users of port or power supply failure
- Redundant power supplies
- Built-in web-based networking management tools
- High speed networking fail-over times of 300 ms or less

- Fanless design
- Extended temperature range - 40 °C to 70 °C

9 Integrated Engineering

An engineering system shall facilitate integration of data through the lifecycle phases of a project from concept through to plant operation and final decommissioning.

The system shall provide a homogenous engineering environment integrating:

- Engineering Management
  - Project structuring (tagging, document numbering)
  - Integrated change management
  - Multi-user and multi-project engineering
  - Bulk engineering (IEA, PAA)
- Basic Engineering
  - Material classes
  - Layouts
  - Flow diagrams, P&ID's,
  - Single line diagrams
  - Consumer lists
  - etc.
- Detailed Design & Configuration
  - Functional charts
  - Graphical Engineering via CFC, SFC and Safety Matrix
  - Circuit drawings
  - Process automation system configuration
  - Cable lists
  - Bill of materials
  - Detailed layouts
  - Isometrics
- Procurement & Manufacturing
  - Materials management (requirements, optimization, tracking)
  - Logistics
  - Quality management (assurance, testing and archiving)
- Construction and Commissioning
  - Installation guides
  - Quality management (assurance, testing and archiving)
  - As build documentation
- Operations
  - Training

- Maintenance support
- Revision
- On-line changes

Process automation system and life cycle engineering tool shall be fully integrated providing automation of engineering workflows.

10 System Configuration

This section specifies the engineering workstation and software tools that shall be available for the initial engineering, configuration, and long-term maintenance of the system.

10.1 General requirements

The engineering workstations shall employ standard PC technology with state-of-the-art hardware based on a Microsoft Windows operating system, and industrial Ethernet communications.

It shall be possible to install more than one engineering workstation in a system.

The engineering system shall be an open system allowing, for example, project data from Microsoft Excel or CAD/CAE tools to be imported. It must be possible to import/export to/from Microsoft Excel for simple manipulation.

Removable storage media shall be provided at each engineering workstation.

It shall be possible to save all database and configuration data on both removable and non-removable media for back up purposes without taking the system off-line.

It shall be possible to provide redundant storage media for configuration database.

The engineering software shall employ an intuitive Microsoft Windows explorer style interface, which will allow the user to manage all aspects of the controller, HMI, network, hardware, and field device configuration. The use of differing, inconsistent user interfaces should be avoided as much as possible.

The system shall offer fast compile and download times.

The system must support archive marking for variables. Marked variables must automatically be archived.

The system must enable data communication with a CAD/CAE system. Support of engineering workflow is required.

The HMI level must be derived from the project created on the engineering station, automatically, to avoid duplicate input of information.

Multi-layer technology must be available for picture designing to enable clear engineering.

The engineering must be supported with graphical resources, pure programming is not acceptable.

The system must enable direct derivation of a picture tree in the OS from the technological/plant hierarchy.

The system shall support hierarchical CFC with graphical block type (chart in chart with compilation).

The system shall be able to detect errors in the configuration, test the connection between two different data types and reject them when applicable.

It must be possible to handle the system engineering even without in-depth knowledge of object-oriented programming.

It must be possible to automatically place and connect all process objects.

The vendor system must be able to display a sequential chart in the OS.

Block programming sources must be accessible to users.

The system must harmonize with SQL, SAP Sybase**,** X Window System and TCP/IP.

Centralized engineering for all components including field devices must be possible.

10.2 Functions of the Central Engineering Workstation

Only one engineering workstation shall be necessary to perform all traditional configuration tasks (control, HMI, batch, and history), fieldbus configuration (transmitters, drives, analyzers etc.), database generation, and editing. However, it shall also be possible to use multiple engineering workstations simultaneously for this work.

The central engineering workstation shall be capable of supporting all of the following functions:

- I/O configuration
- DCS hardware configuration (controller, operator stations)
- Configuration of plant and field communication networks
- Fieldbus instrument configuration and maintenance
- Configuration of drives, weighing scales and motor management equipment
- Configuration of continuous and sequential control operations
- Configuration of the plant process structure / hierarchy, for example, compliant to S88
- Configuration of fail-safe (Safety System) Functions
- HMI graphics display generation and modification
- Tag logging (archive) configuration
- Configuration of historical and real-time trends
- Management of alarm and event configuration
- Report creation, generation and modification
- Configuration of user security and access privileges
- Process object view with test mode
- Data communication with a CAD/CAE system
- The operator shall be able to perform their desired picture assembly online.
- Batch Configuration & Planning (Recipes, Procedures, Formulas etc.)
- Asset Management configuration

- Access to external files and programs such as Microsoft Excel
- System diagnostics
- Servers, clients and keyboard plant area assignments
- A controller simulator tool to enable logic debugging and testing w/o requiring any hardware.
- It should be possible to protect the engineering project via a user specific password.

10.3 Object Oriented Engineering Tools

Object-oriented configuration tools shall be provided to aid in system configuration. It shall be possible to configure both control and HMI aspects at the same time from this tool for one or multiple process objects. The tool shall include a spreadsheet style interface for configuration which supports ease-of-use with functions such as copy/paste, search and replace, sort by column, and connection with Microsoft Excel/Access. The following parameters shall be configurable from this interface:

- Control: Loop identifier, Alarm limits, Tuning constants, Descriptors, Engineering Units, I/O assignment.
- HMI: Alarm Priorities, Alarm Message Text, HMI Symbol assignment, tag Archive rates.

The engineering system shall have a uniform database ensuring that data, which has been entered once by the user, shall be available to all tools throughout the system, thus ensuring that there is a single point of entry for the system database.

10.4 Optimization of the Run Sequence

The system shall be capable of naming processing cycles or runtime groups for optimization of the run sequence / runtime group.

It must be possible to change the processing sequence of the function blocks.

10.5 Bulk Engineering Capabilities

The system shall provide tools for bulk editing of the configuration and to facilitate easy duplication of standard control elements (those provided standard by the system or created custom by the user). The duplication tool shall support generation of instance-specific copies via an export / copy / import routine that utilizes a spread-sheet style tool for configuration.

Duplication and instantiation of the following element types shall be supported:

- Function Blocks
- Function Block Charts (control modules)
- An entire unit of equipment
- An entire process area
- SFCs

The tool shall support cloning of process control elements through the import of configuration data from an external file.

The tool shall also provide a menu-guided process for defining reproducible elements and for selecting instance-specific attributes (such as tag name or configuration area) of each individual element.

A user interface similar to a spreadsheet shall be provided for cloning elements (such as motors, valves and PID controllers) and for the configuration of their instance-specific properties.

10.6 Standard Process Automation Library for Controller and HMI

A library of standard prebuilt control algorithms for process control shall be available along with their associated HMI faceplates/symbols.
Optional Industry specific libraries shall be available. The standard library shall consist of the following control strategies and pre-engineered symbols/faceplates at minimum:

- Standard PID controller
- Cascade PID controller
- Ratio controller
- Split range controller
- Manual loader
- Totalizer for solids and liquids
- Digital value monitoring with alarming
- Analog value monitoring with alarming
- Motor (Start / Stop) with interlocks
- Motor – two speed
- Motor – forward / reversing
- Valve (On/Off) with 1 or 2 feedback signals
- Valve (On/Off) with interlocks
- Motorized valve control

10.7 Configuration Structure

The application shall be viewable and configurable in a hierarchy which groups configuration elements according to the plant or process structure. This plant hierarchy shall be capable of directly representing the process model and the physical layout of the process. It shall be used to automatically derive the display hierarchy in the operator interface and to generate the dynamic elements of process graphics.

For maximum flexibility in structuring the controller program, the system shall support the creation of a configuration hierarchy that is at least eight levels deep.

10.8 Copy / Paste

The system shall support *copy and paste* of all configuration elements contained within the hierarchical configuration structure including:

- Control Modules (Function Blocks or Charts)
- SFCs
- Process Graphics

The system shall support the ability to copy and paste multiple levels of the hierarchy in a single step (tree copy) allowing entire process areas or units to be copied and modified with minimal engineering effort.

10.9 Concurrent Engineering

The system shall support concurrent engineering practices whereby multiple engineers can work on the same application via a networked environment or via a “check-in / check-out” style for configuration locally on different PCs.

10.10 Documenting the Configuration

Tools shall be available for automatically documenting the configuration and project data.

The system shall be able to display the connections between individual charts in the automatic documentation.

10.11 Online Configuration Changes

The system shall support making changes to the controller, I/O, HMI, Batch, and Communication network while online without interrupting operations.

10.12 Change Management (General)

The engineering station (ES) shall support versioning.

Configuration additions, changes, and deletions shall automatically update all modules and tags affected by the change.

Configuration changes shall follow a prompt-validation sequence requiring a final acknowledgment step before the change is downloaded to the on-line system. An

option shall be provided to allow the user to view a detailed report of changes as part of the download confirmation process.

When configuration data are compiled or downloaded to the system, invalid configuration entries shall be identified and the parameters affected shall be indicated.

It shall be possible to change, delete, and add any independent loop in the controller without affecting the other loops.

In the multi-project mode, the system shall support updating of blocks from the master data library in libraries of the individual projects.

10.13 Multilingual Engineering Environment

At a minimum, the English, German, French, Italian, Spanish and Portuguese languages shall be supported by a single version of software. The user shall be able to toggle between the different supported languages in the Engineering and Operator runtime environment without having to recompile the program.

10.14 System Management

System management shall be performed centrally. The following main functions shall be available:

- Inventory management of all hardware and software
  - Ability to read and access inventory data from servers, operator stations, engineering stations, controllers, communication switches, and remote I/O
  - Version and license management of hardware and software
  - Reporting and export of system configuration to Excel
- Software installation management
  - Updating of servers and operator stations
  - Preparation of rollouts for servers and operator stations
  - Status / condition monitoring of target stations, disabling stations for updating, re-enabling stations for use

11 Configuration of Control Strategy

11.1 Custom Function Blocks

The system shall allow users to create their own custom function blocks from scratch using ladder logic, structured control language or other. These custom function blocks should be able to be added to the application library for reuse throughout the project.

Custom function blocks shall be used in the application just like a standard function block (for example they can be embedded in CFCs or connected to standard function blocks)

Custom function blocks shall have the capability of being password protected so that access to proprietary intellectual property may be protected in the field.

There shall be no practical limit to the number of custom objects that a user can create and download is only limited by the memory capacity of the target controller.

11.2 Interconnection of Function Blocks and Control Modules

All parameters contained in a control module (composite of multiple function blocks) shall be able to be directly connected to another control module without the need for additional parameter function blocks.

The system shall support auto routing which allows function blocks which are located anywhere in the configuration to be connected quickly by two mouse clicks.

The system shall prevent the user from connecting together function block parameters which have different types (real, Boolean, string etc).

11.3 Process and Equipment Interlocks

For ease of use and to minimize engineering costs, it shall be possible to configure device interlocks graphically via simple point and click operations between function blocks. It shall not be acceptable to require the user to program the interlocks using a text-based script-editor.

11.4 Testing and Commissioning

All configuration tools shall have test and commissioning functions, for example, it shall be possible to display and modify the value of a function block input or output parameter during operation, and with SFCs, to display step conditions and transitions during operation.

From the engineering environment, the user shall be able to view real-time input and output values from the control system within a spreadsheet-style view.

The user shall be able to create Dynamic Trend Displays from the engineering environment to monitor selected real-time input and output values from the control strategy.

It shall be possible to disable the execution of a configured module or force specific values (i.e. hardwired I/O signals) to override the actual signal, all without affecting other modules that may be running in the same controller.

11.5 Configuration / Change Management

Change tracking of Function Blocks

Each function block or chart shall have a unique Date/Time stamp which indicates when it was last modified. This information shall be displayable as an object property so that it is viewable directly from the engineering tool.

Function blocks / Charts shall support the assignment of a unique version number and author. This information shall be displayable as an object property so that it is viewable directly from the engineering tool.

Comparison Tool (Version Cross Manager)

An optional tool shall be available to perform a detailed comparison of two applications or versions of an application. This tool shall use a Microsoft Windows Explorer-like interface to graphically highlight what elements of a configuration are different (CFCs, SFCs, Function Block types, application cycle, etc). By selecting a “flagged” element, the user can dive deeper to determine exactly what is different (such as an Alarm Limit or Tuning Parameter).

The comparison tool should be able to identify differences in the following elements at minimum:

- Application Program (Function Blocks, Charts, SFC, hierarchy / layout)
- Hardware Configuration
- Communication / Network Configuration
- Alarms
- SFC details (Steps, Transitions and Properties)

Project-Specific Libraries

The system shall support creation of a project-specific library which contains only those standard function blocks, charts, and custom function blocks developed by the user that have been approved for use on the project. During configuration all other system libraries can be hidden to ensure that the project team uses only the “project-approved” elements during the application development phase.

Central Management of SFCs

The system shall support central management of SFCs by providing “SFC Types”, which allow a single sequential function chart (e.g. Reactor Heat Phase) to be copied and reused throughout an application. Making a change to one instance of the SFC shall result in the automatic update of all other instances in the configuration, thus saving engineering time and minimizing the chance of creating inconsistencies in the application.

Change Log

An optional tool shall be available for use on the Engineering workstation to enforce user access control for execution of protected actions (such as downloading a configuration change to the controller) and to allow recording of comments (detailed reason for change). Information will be recorded in a change log file, which shall be continuously updated with each new change. The change log shall be capable of being reviewed at a later point in time.

Assistants

A wizard shall be available to generate all blocks required for the diagnostics of I/O modules and field devices.

Object naming

Object naming shall support at least 16 alphanumeric characters, and users shall be able to change an object’s tag name without deleting and re-adding the object or any references to it, for example, SFC charts, process pictures or tag logging archives.

11.6 Database Reporting and Modification Utilities

Global Search Utility

Utilities shall be provided for global searching of the database. These utilities shall be under system access control.

Cross Reference Data Listings

The system shall be capable of generating listings containing the following fields:

- Tag ID
- Tag descriptor
- Point type
- Hardware address

It shall be possible to perform the following functions on the above list:

- Sort alphanumerically by any field
- Filter by any field
- Print, display and store to media
- Export Data

The above listings shall be available for all devices in the system.

12 Configuration and Management of Field Devices

A field device management tool shall be available to configure, parameterize, commission, and view diagnostics for intelligent field devices remotely (via a local station in the field), or from a central engineering station.

This single tool shall provide a uniform display of device parameters and functions for all supported devices regardless of their communication link, for example PROFIBUS-DP, PROFIBUS-PA, the HART protocol, Foundation Fieldbus H1 and PROFINET.

The tool shall support the online addition of field devices to the network without interrupting operation of the system.

The management tool shall support configuration and management of devices from third-party manufacturers as well as those from the system vendor.

The system shall offer the option to connect modules that are outside the standard range.

The system shall offer the option to connect fail-safe fieldbus instruments.

The system offers ready solutions for controlling and diagnosing drives via the fieldbus.

The vendor system must provide a stable power supply for HART modules.

It must be possible to configure interlocks without a programming language.

12.1 Centralized Engineering, Maintenance & Diagnostics

The field device management tool shall have the capability of communicating with remote field devices from a central location using routing. The routing functionality shall allow communication to pass between different networks or subnets of the system transparently, so that the user can communicate with remote devices without having to connect locally to them in the field.

12.2 Communication modes

The field device management tool shall support the following modes of communication at a minimum:

- PROFIBUS DP Interface
- PROFIBUS PA Interface
- HART Interface
- HART Multiplexer
- HART Modem
- Foundation Fieldbus Interface
- PROFINET

12.3 Functions of the Field Device Management Tool

The tool shall provide the following main functions:

- Assignment / Configuration of Slave (network) addresses
- Device adjustment and modification
- Device comparison
- Plausibility testing
- Simulation, including a choice of predefined simulation routines such as ramp up, down, randomize, etc.
- Automatic diagnostics
- Management and commissioning
- Online monitoring of selected values, alarms, and status signals
- Life list for the automatic detection of existing field devices with the ability to:
  - Open a device configuration screen directly from the life list
  - Add devices from the life list to the application
  - Configuration of field instrumentation from the life list (for fieldbus and for HART devices)
- The vendor system shall support HART instruments in the life list
- Import/Export capability for field device data exchange with other projects or other tools.
- Export of device status information
- Document management to allow online access to up to 10 documents per device
- Change log
- Integration of FDI device data packets

12.4 Field Device Management Displays

The tool shall have a graphical user interface supporting several different views of the field devices:

- Hardware project view
- Process device network view – Displays device information, including diagnostic status, grouped according to the network topology
- Process device plant view – Displays device information, including diagnostic status, for all devices in the system from all configured networks
- Field device parameter view – Displays detailed device parameter information in a tabular format. This view shall support display of the following parameter information: Parameter Name, Value, Unit, and Status (Initial Value, Changed, or Invalid)

12.5 Comparison of Online and Offline Device Data

The tool shall support the ability to do a direct comparison of the online and offline device data. The comparison shall be displayed in a side-by-side format with the differences highlighted automatically by the tool.

12.6 Updating Device Profiles and Adding New Devices

The device management tool shall support the easy integration of new field devices and device driver updates of existing devices purchased from the system manufacturer or from third-party manufacturers. The device description files and drivers required for updating the management tool can be downloaded from the manufacturer's internet site. Device description files will utilize the Electronic Device Description Language (EDDL) format (IEC 61804-4).

12.7 Device Diagnostic States

The management tool shall support the determination and display of the following diagnostic states at a minimum:

Communication States: Unchecked, Fault, Good

Device Status: Unchecked, Configuration Error, Fault, Maintenance Required, Maintenance Recommended, Simulation or Manual Operation, Process Error, Good

12.8 Role-based User Access & Security

The tool shall provide at least two different sets of user access and authorization privileges. At minimum the following users and sets of access privileges shall be provided

Maintenance Engineer – Can modify only operational data (parameter changes)

Specialist - Can modify all configurable data. Includes the optional definition of a password for access protection

12.9 Logging Tool

For troubleshooting purposes, the device management tool shall provide an integrated logging function. The log shall provide the ability to activate and choose which types of messages are displayed within the tool and to be saved to file for later review.

The following types of messages (selectable) shall be recorded as part of the logging function:

- Errors
- Warnings
- Communication Messages
- Details

13 Configuration of the Operator Interface

The workstation for Human Machine Interface (HMI) shall provide an object-based process graphics engine, which is capable of providing process visualization and control. A standard utility shall be provided that is able to generate and modify user-defined color graphics. It shall use the same tag IDs that are used in the process database to access real-time variables from any database. It shall be subject to system access protection.

The vendor system shall offer a wireless, mobile input medium.

The number of simultaneously opened windows may not be limited.

13.1 Capabilities of the Graphics Development Tools

The workstation shall include easy to use drawing tools, graphic palettes, and standard graphic object libraries.

The graphics system should provide *wizards* to help the user with multi-step configuration operations including but not limited to: exiting the HMI application and/or Microsoft Windows, dynamic language switching, screen navigation, calling up an external application, faceplate call-up, and connecting a symbol to a process object.

The dynamic properties of each graphic object, including fill level, fill color, text, shall be easily modifiable by assignment on the object's property sheet.

The graphics system shall support configuration of separate scan / refresh rates for individual graphical elements (symbol, process value etc) to allow for optimizing the system load.

The workstation shall provide support for standard Microsoft Windows functionality such as: cut, copy and paste, drag and drop, grouping, ungrouping, and layering of objects. The cut, copy, and paste functionality shall allow the user to include windows clipboard content.

The graphics system shall include a selectable grid to align objects vertically, horizontally, left, right, top, bottom, and automatically space objects with equal horizontal or vertical distance between them. Tools shall also be provided to rotate and flip objects horizontally and vertically.

The graphics subsystem shall provide up to 32 graphical layers which can be individually enabled/disabled (like a CAD Drawing Package) to facilitate the drawing of complex pictures. The following layering capabilities shall be provided:

- Ability to promote / demote objects between layers
- Zoom functionality while creating pictures, including the ability to *rubber-band* specific areas of interest
- Minimum desktop size of 1920 by 1200 pixels

13.2 Standard Graphic Elements provided by the System

Standard graphic elements provided by the system should include but not be limited to: Lines, polygon curves, polylines, circles, arcs, ellipses, rectangles, polygons, static text, OLE objects, ActiveX objects, input and output fields, bars, graphic picture objects (bitmap BMP, Microsoft Windows Meta File WMF, and Enhanced Microsoft Windows Meta File EMF), status displays, text lists, 3D bars, buttons, check boxes, radio boxes, and sliders.

The system must support the use of vector graphic files which can be adapted to the respective resolution of the commercially available monitors and mobile devices and can be continuously increased or decreased.

The system shall provide pre-configured *smart* control objects to represent clocks, gauges, tables, application windows, alarm windows, and trend windows.

The workstation shall be supplied with a full library of process-oriented objects for the development of process graphics including but not limited to: pipes, motors, valves, pumps, tanks, fans, indicators, sensors, conveyors, and electrical symbols. These objects shall be provided in various formats (static, capable of being dynamically linked to the control strategy, 2-D, and 3-D).

13.3 Dynamic HMI Symbols for the Control Library

Pre-engineered graphics symbols shall be provided for all process control elements in the standard control library (PID Controller, Valves, Motors, etc). These pre-engineered symbols shall be designed to call up their associated faceplate and to represent the dynamic behaviors of the underlying control element, without requiring any additional configuration effort.

The workstation shall allow the user to create libraries of custom and composite symbols. Library management shall be an integral part of the system.

The system shall allow identical handling of all safety- and non-safety-related process tags (process variables) in the OS (visualization, operator control, monitoring, etc.).

13.4 Global HMI Symbols

The system shall support the creation of global HMI symbols for representation of process control elements. Edits to one instance of a global symbol shall be propagated automatically via a wizard to all other instances of the symbol in the application without manual reconfiguration.

13.5 HMI Faceplates

Faceplates shall be generated automatically by the system for each function block / chart provided in the process control library (PID Controller, Motor etc).

The User shall not be required to individually configure a faceplate detail display for each instance of a process object or control module.

Faceplates shall be linked to a corresponding HMI symbol such as a motor or valve. The symbol shall be programmed automatically by the system to call-up the appropriate faceplate without requiring any manual engineering steps.

A Faceplate list (Tag List) shall be created automatically by the system. This tag list will allow an operator to call up a faceplate by selecting it from a list of tag names.

The system shall provide a dedicated Faceplate Designer utility to facilitate easy creation of custom faceplates.

It must be possible to simultaneously open 3 faceplate instances on the OS.

13.6 SFC Visualization

To minimize engineering costs, the system shall be capable of automatically generating HMI representations of SFCs (aka SFC Visualization) directly from the control strategy, without additional engineering. These screens shall allow operators to monitor the status and interact with an SFC directly from an operator console.

SFC Status Displays

The system shall provide a standard SFC Status display object which will provide an overview of the status of the area-relevant SFCs. Additional information including the SFC Visualization faceplate shall be accessible from this status display.

13.7 Automatic Creation of Process Graphics

HMI displays, including the dynamic elements used to represent function blocks (such as motors, valves and PID Controllers), shall be generated automatically from the controller configuration. No manual engineering shall be required to place the dynamic elements on the displays or to link them to the controller configuration.

The user interface should support automatic creation of static process pictures.

13.8 Automatic Creation of Display Navigation

A hierarchical navigation scheme shall be created automatically by the system for operator call-up of process pictures.

13.9 Change Management

To simplify change management and limit configuration errors to a minimum, the system must support automatic updating of all references to changes (Change Management) in a function block (including process graphics, faceplates, archives and scripts), for example, by changing the instance name of the function block.

13.10 HMI Scripting

The HMI development environment shall support the ability to customize the application through the use of powerful scripting languages. The system shall support the following languages

- ANSI C
- Scripts

The programming environment shall support the following functions:

- Ability to access properties and methods of all ActiveX controls included with the application or provided by a third-party
- Ability to easily establish connections to other applications / databases (such as Microsoft Excel and SQL databases)
- To execute system functions such as initiating a report or generating an operator message
- To define custom menu entries or configuration dialogs
- User friendly editor with debugging support
- Search and replace function to facilitate text modifications
- A windows tree / list view presentation techniques to facilitate the display, creation, and editing of program scripts
- Ability to have multiple functions or actions open simultaneously, and be able to drag and drop code between them

The programming environment shall permit user developed functions and/or libraries to be easily loaded and called.

13.11 HMI Database

The system shall have the flexibility for the user to configure how many levels of the controller structure (up to five) should be included in the HMI tag name.

The database system shall support both internal (computational) and external tags (real world). The database system shall support the following tag types/storage formats: binary, signed 8-bit, unsigned 8-bit, signed 16-bit, unsigned 16-bit, signed 32-bit, unsigned 32-bit, 32-bit IEEE 754 floating point, 64-bit IEEE 754 floating point, 8-bit character text, 16-bit character text, raw (user definable) and structured (template) tags.

Tag IDs shall be unique throughout the system and access to all tag parameters for configuration shall be available directly by tag ID.

The system shall provide the capability to define free-format alphanumeric descriptors for each state of a multi-state device, for example, open, closed, travel, and fault for a motor operated valve (MOV).

Configuration and archive data shall be stored in a relational database, which can be read using ODBC (open database connectivity) and Standard Query Language (SQL).

The vendor system shall provide consistent archives following a system failure.

The project archive shall contain all HMI segments. Additional work steps are not accepted.

13.12 HMI Text Library

To support localization of multilingual applications the system shall provide a text library of terminology which can be configured to contain translations for any number of languages defined by the user. This text library shall be accessible by the operator interface during runtime to allow messages and text strings to be presented in the local language. The text library shall be capable of being exported and imported to facilitate easy configuration using Microsoft Excel.

13.13 Concurrent configuration of HMI

Concurrent configuration of the HMI shall be possible by multiple users.

13.14 Multi-version support

In order to support system extensions and phased upgrades the HMI shall support different versioned function blocks and control modules in controllers. HMI faceplates shall be common for the different versioned function blocks and control modules.

14 Operator Interface Architecture and Hardware

14.1 Architecture

The Operator Interface shall be flexible to cover all possible applications from single user system (single station) to distributed client / server architectures. The architecture shall promote the use of multiple server and multiple client configurations.

The system shall be scalable, enabling the user to expand an existing installation by a simple license upgrade.

An intrinsically safe operator panel, which can be located up to 200 m from its PC, shall be available for use in potentially explosive atmospheres. (EEx-i).

The system shall allow multiple clients to access up to 18 servers or 182 redundant pairs of servers. Each server or pair of servers shall be able to communicate with up to 40 clients.

Any server computer shall be able to be dedicated to specific process functionality (i.e. Alarm Service, Historical Data Collection, etc.)

Archiving of process variables should be possible on single stations, OS Servers and a dedicated historical archive server.

In general it should be possible to add a redundant OS Server or historical archive server to a non-redundant structure at any time.

All clients shall have complete visibility to all servers and the historical archive server and all servers shall have visibility at the peer level.

The software shall promote portability of applications between computers without any redevelopment or modification.

It shall be possible for the user to monitor and control the process from client or server. This includes but is not limited to:

- View the same or different displays simultaneously
- Make process adjustments and acknowledge alarms
- View alarms, events, trends, and reports

The development and runtime environments shall be decoupled allowing the user to configure run-time only clients without any development capabilities.

For small systems it should be possible to combine all system engineering functions, the Operator Interface, Archiving, Batch and Controller on one PC.

14.2 PC Platforms

The Operator Interface consoles shall utilize standard PC technology with state-of-the-art hardware based on a Microsoft Windows operating system, and industrial Ethernet communications.

The system shall support the operating systems Microsoft Windows 7/Windows 2008 Server and Windows 10/Windows 2012 Server.

It shall be possible to swap out the complete project data onto external disks for long-term data storage.

For servers the hardware shall support up to RAID XX hard disc redundancy-

All operator and server equipment shall have ECC memory support.

Processors shall be of at least 4. Generation Intel with selectable performance available from i3 to the i7/XEON.

PC components shall be suitably industrialized suitable for control room and/or process area installation.

Higher performance PCs, such as for servers, shall have 19" rack mount form factor.

Lower performance PC's, such as for clients, shall be available in both 19" rack mount or in compact design suitable for field mounting.

The operator interface shall be available in local operated panel (LOP) form factor with high resolution touch screen and integrated PC components.

14.3 Monitors

Monitors for operator stations shall be as follows or better:

- Diagonal measurement 21”
- 1920 x 1200 resolution
- 32,000 colors

14.4 Multi Monitor operation

The system shall support quad graphics cards with a resolution of up to 1920x1200 pixels.

If multi-VGA cards are used, each OS client shall be able to drive between two to four monitors, but with a corresponding reduction in the number of clients per server. The multi-monitor workstation shall allow user configurable layouts. It shall be possible to dedicate either one or both monitors to the operator interface. Additionally, it shall be possible to use the second monitor to view other applications without interfering with the viewing of operator process graphics and displays.

14.5 Printers

Display Hardcopy

The OS shall be able to generate a hardcopy of any active display.

The system shall support both full color and black and white copies for all displays.

The system shall support local or networked printers.

Laser printers shall be supported.

14.6 Time Synchronization with Control System

The Operator Interface shall be capable of synchronizing its time with the control system so that there is no more than a 20 ms deviation between input/output events in the field and events occurring and being time stamped at the HMI level.

System time will be based on UTC. However means shall be provided to display time based on the local time zone setting within the Microsoft Windows operating system.

The System shall support connection to a highly accurate time source such as GPS (Global Positioning System) or DCF77 which can be used as the time master for the system.

Date and time synchronization shall be possible anywhere in the world using a satellite source such as GPS (Global Positioning System).

14.7 Web / Thin Client HMI Architecture

The system shall support web-based HMI functionality from an Microsoft Internet Explorer browser window via an Intranet/Internet or TCP/IP connection to the system's HMI web server.

HMI Web Server

The HMI Web server shall be capable of supporting access for up to 100 web clients simultaneously.

HMI Web Client

Web Clients shall not require a full installation of HMI software, but should be operational simply by loading Microsoft Internet Explorer in combination with selected plug-ins. Plug-ins shall be loadable over the internet.

Web client for mobile devices

The System shall allow mobile operation and monitoring with all commercially available mobile devices. No software installation on the end devices is required and the mobile devices have to support simply HTML 5 compatible browsers.

Creating HMI Displays for Web /Thin Client Operation

HMI graphics for display on a Web client shall be automatically created by “publication” of the application into a form suitable for presentation by Microsoft Internet Explorer.

Web / Thin Client Operation

The Web client will utilize operator graphics similar to those on the main control system with access privileges based on security/login information used in the main control system.

In order to support the operator, the Web client must be able to signal acoustic alarms in the event of an error message.

Based on password access, web client users will be able to perform the following standard operator actions at a minimum:

- Setpoint changes
- Automatic/manual loop status changes
- Alarm acknowledgement.

Security of the main Operator Station Web server is maintained by end user limiting access by firewall and password authorization to their plant/corporate network.

15 Operator Interface for Process Control and Monitoring (Runtime)

15.1 General

All displays and graphics that show real time data shall be automatically updated when the display or graphic is on a screen. Updates shall not require operator initiation.

Operators shall be able to easily access specific displays and graphics by pressing dedicated function keys or overview buttons, selecting from a hierarchical list of displays in directories or menus, or by selecting from an alphabetical listing of all displays.

It shall be possible to move between related displays and graphics of different detail levels or of the same detail level with a maximum of two operator actions.

Special indication shall be used to indicate that a value is invalid.

The system shall provide an overview of the alarm status of all areas to which the operator has access, no matter which graphic is displayed.

The vendor system must provide information regarding the violation of performance limits (memory, cycle time) during download.

It must be possible to modify operation enable for each instance (relating to parameter type).

The system shall allow plant operation and data communication via the Intranet/Internet (use of Internet browsers) based on the configuration.

15.2 Graphics Subsystem

The graphics subsystem shall allow the operator to trigger a control action based on one or two user inputs. At a minimum, the control action will be triggered upon:

- Mouse button press
- Mouse button release
- Keystroke event

The operator shall enter data by either:

- Direct data entry
- Use of up/down keys
- A scrollbar or slider

The operator can browse in the picture hierarchy at the top of the screen to bring up the desired display.

User configurable buttons or screen targets to select operational functions or displays with a single entry shall be provided. Popup displays shall be movable and expandable by the operator.

All operator triggered control actions shall be logged within the message archive system.

It shall be possible to change control assignments to allow control of any plant area from any operator workstation by using the appropriate access password.

An SFC visualization display shall be available showing the step and transition displays with step comments or the dynamic step conditions.

For safety systems that have been configured using the Safety Matrix, a Visualization screen shall be available to view the status of the cause and effects matrix online.

15.3 Faceplates

Faceplates shall be provided with the system to allow for control and monitoring of both regulatory and discrete control algorithms.

Faceplates shall support the display of the following information as applicable:

- Tag ID.
- Tag descriptor.
- Process input, setpoint, and output values displayed numerically with engineering units.
- Process input, setpoint, and output in bar graph representation.
- Auto/manual mode and remote/local setpoint status.
- Visual indication for alarm status.
- Symbolic and alphanumeric indication of discrete states both for two state devices and multi-state devices.

Faceplates shall be defined to pop-up when the appropriate location on a process graphic (such as a symbol) is selected with the mouse.

Regulatory Control

Faceplates shall show dynamic process and status information about a single control loop. It shall be possible to perform the following control actions from a faceplate:

- Change control block mode.
- Change setpoint and other operator settable parameters.
- Adjust outputs in manual mode

Discrete Control

Single faceplates shall be provided for control and indication of multi-state devices. For example, a motor operated valve shall indicate open, closed, intermediate position, and fault. An operator shall be able to operate the device (start, stop, open, close) from the faceplate.

15.4 Process Graphic Displays

It shall be possible to place a new graphic in service without interrupting an operator's ability to control the plant.

All control, monitoring, and status attributes of any tag shall be displayable on graphics. For analog points this requirement includes measurement, setpoint, alarm limits, and output. For digital points this requirement includes input and output status. Status information includes: alarm status, control mode, and control status.

Numeric data shall be configurable on an individual basis. If the decimal point is not used, it shall be suppressed.

It shall be possible for each state of a multi-state device to be indicated by a unique foreground/background color combination.

It shall be possible for inactive alarm or status messages to be invisible to the operator.

Symbolic representation of data on the graphics shall be performed by color changes (foreground and background independently), and flashing in any combination.

The system shall support programming of tooltips which will display a configurable text message to an operator when he hovers over the element with his mouse.

It shall be possible to configure an area on the screen that calls up other displays.

It shall be possible for the operator to zoom in and out during runtime.

15.5 Enhanced Process Graphics

Plant managers, shift manager, operators and field operators shall be supported by enhanced process graphics. These shall increases the situational awareness of the operators, resulting in safer and more reliable operations providing a high-performance HMIs.

In addition to complying with ISO 11064-5 to provide an ergonomic environment for operators, the system shall provide enhanced functionality detailed in the EEMUA 201, ISA S201 (draft) and ASM Consortium’s “Effective Operator Display Graphics guidelines”.

The enhanced process graphics shall allow operators to rapidly recognize abnormalities and provide clear overviews of plant status and performance.

Ergonomic design for operator’s shall be improved with features such as:

- Analog displays for "pattern support such as vertical and horizontal bar charts with expanding information windows
- Trend displays with gradient and flexible axis for assessing situations and deciding on operating strategy
- Representation of information instead of data for example using spider diagrams (polar star charts) for KPI‘s and process status
- Fast navigation features with jump to process control loops of tags for operators

15.6 Screen Composition Favorites

The system shall support the operator's ability to save specific screen compositions or layouts for call up at a future time. A favorite screen composition can consist of a process graphic with any number of specific device faceplates, trends etc. overlaid on the screen and positioned in specific locations of the display.

15.7 Dynamic Language Switching

The Operator Interface shall provide the user with the capability to easily switch between languages and international character sets while online. Conversion between English, German, French, Italian, Spanish and Portuguese shall be supported at a minimum. Re-programming, recompilation, or reconfiguration of the HMI software application shall not be necessary to achieve this functionality.

15.8 Access Control

The access control configuration tool shall provide an easy to use, simple interface, which offers full support for standard Microsoft Windows techniques such as copy, cut and paste, as well as drag and drop.

The system shall allow an individual's authorization to be programmatically modified and/or verified as part of the Control Logic/Scripting requirements.

The system security shall allow the configuration of authorization groups whereby individual users can be assigned to permission groups.

The access control tool shall allow the configuration of process area specific security for up to 256 different process areas.

The system shall support the configuration of custom security and access authorization levels up to a total of 999.

Default Security Levels

The OS system security shall provide different security levels to allow the access and interaction with the process to be controlled. At a minimum the following access levels should be pre-defined:

- User Administration
- Ability to View alarms and call-up Displays from a particular area of the plant
- Ability to Navigate through the system
- Process Monitor - Ability to view the process in Monitor Only mode
- Process Control (Basic) - Ability to Control the Process by sending commands, acknowledging alarms and changing setpoints etc.
- Process Control (Advanced) - Ability to modify alarm limits, PID tuning coefficients etc.
- Ability to trigger reports
- Ability to control archiving / storage

Advanced Access Control

The Operator Interface shall support the optional use of a chip card readers or a fingerprint mouse (biometric signature) to ensure unique user identification.

Global Security

The system shall support an optional common security system whereby the same login / password is used for the Microsoft Windows operating system, the engineering environment, the HMI and for the Batch system.

15.9 Expandability and Extensibility

The system shall be able to collect data from multiple data servers, including other OPC-enabled process and control systems.

It shall be possible to exchange system data with other third-party software that are compatible with Microsoft Windows operating systems.

The OS system shall be based on an open architecture and support extensibility thorough the use of:

- COM/DCOM
- ODBC (Open Database Connectivity)
- OCX / ActiveX Controls
- OLE (Object Linking and Embedding)
- OPC (OLE for Process Control) Data Access Protocol (DA)
- OPC Historical Data Access Protocol (HDA)
- OPC Alarms & Events Protocol (AE)
- OPC Historical Alarms & Events (HAE)
- OPC UA

The OS system functionality shall be expandable via the optional add-ons including, but not limited to:

- User programmed ActiveX objects
- Automatic event driven email messaging of real-time information
- Event triggered display of live process images
- Long term historical media-based data storage
- Configurable messenger functions such as SMS, E-mail, Pager

16 Alarms, Events, and Messages

16.1 General

The alarm system shall provide complete alarm and event management with a user definable message structure.

The alarm system shall support definition of up to 16 message sub-classes and 16 message types.

Alarms must be assigned a time stamp based on the execution cycle in the controller.

The vendor system shall support a time stamp resolution of 1 ms for binary inputs.

The alarm system shall alarm any change of state that the system detects including:

- Any violation of limits
- Any change of state of a device connected to the system including all of its peripherals
- The failure of any communications channel used by the system
- The failure of system's hardware, which results in an automatic fail-over of the system's functions from the active to standby device.

The alarm system shall display alarm messages in a manner to facilitate easy interpretation of the current alarm status including but not limited to:

- Different text color and background color for those points that are in alarm, those that have been acknowledged, and those that are no longer in alarm
- Flashing of the current alarm message(s) in the alarm list
- Alarms that have been automatically hidden by the system or manually by the operator
- The system shall provide the option of displaying alarms in ascending or descending temporal order.

The vendor system shall provide a configurable, OS-spanning horn design.

The vendor system shall provide automatic alarm OR'ing in the plant overview, without additional configuration.

The vendor system shall support more than 4 alarm priorities and more than 5 permission levels.

The alarm system shall conform to the upcoming IEC 62682 standard 'Management of Alarm Systems for the Process Industries'.

The system shall allow entering and storing of a detailed description for an alarm. With it the stored error description can be displayed with an operator action.

Alarm Acknowledgement

The alarm system shall provide capability to acknowledge an alarm message when a data point enters and / or exits alarm state. The system shall permit alarm acknowledgement including but not limited to:

- For an individual alarm from the overview
- For a filtered grouping of alarms from a summary list
- From the device faceplate
- From a process display (screen acknowledge)

Alarm acknowledgement from one operator station shall be automatically synchronized to other stations to provide global acknowledgement capability.

The operator name shall be saved when alarms are acknowledged.

The system shall offer the option to disable or enable messages via a second set of keys.

Filtering of Alarms

The alarm system shall provide filtering to control the behavior of the alarm display screens. The filtering attributes shall include but not be limited to:

- Date
- Time
- Alarm class
- Alarm type
- Alarm priority
- Status (in alarm, out of alarm, or acknowledged)
- Tag name
- Area

Alarm Status Symbols

The alarm system shall provide the ability to condense and present system alarming status in the form of a standard alarm status symbol (i.e. alarm group display). The group display shall be capable of indicating the status of an individual device or of an entire process area. When used to represent the status of a process area, the group display shall form a logical *OR'ing* together of the alarm states from all devices in the process area.

The group display shall include the following standard alarm categories at minimum, which will each be represented in the symbol with a different color and text representation:

- Alarm
- Warning
- System alarm
- Operator message (operator action required)
- Suppressed alarm state

16.2 Alarm Priorities

To allow for segregation of alarms based on criticality, the system shall support the assignment of individual alarm conditions to one of at least 16 different alarm priorities.

16.3 Categorizing Alarms and Messages

Process and designated system alarms shall be annunciated, displayed and stored in history files. Normal plant operator actions, events and normal system actions and events shall not be alarmed; however, they shall be stored in centralized history files.

Alarms and messages shall be grouped to allow the user to readily identify and respond to alarms and conditions (e.g., in priority sequence) in his area of responsibility.

For any process alarm, it shall be possible, by no more than one operator action, for an operator to access a display from which he may take corrective action.

The system shall support the ability to display the highest priority, most recent, alarm at all times.

Operator Actions

The system shall automatically store all operator actions that affect process control parameters or alarm acknowledgment in centralized history files, including:

- Enable/disable/acknowledge/suppress/lock/shelve alarms
- Change mode of controllers
- Change setpoint of controllers
- Changes to alarm limits.
- Changes to tuning parameters

Engineer Actions

The system shall provide the ability for Engineering actions that change the control and monitoring of the process to be stored in a log file along with a comment. These actions shall include the following:

- Download of controller configuration
- Online/Test Mode
- Download of Batch / Operator Station Configuration

16.4 Process Alarm Initiation

It shall be possible to initiate process alarms by configuring alarm attributes of any process I/O point or any calculated point.

For analog tags, the configurable triggers for process alarms shall include:

- Process variable high limit exceeded
- Process variable high high limit exceeded
- Process variable low limit exceeded
- Process variable low low limit exceeded
- Process variable deviation from setpoint
- Process variable invalid value (bad quality)

For digital tags, the configurable triggers for process alarms shall include

- specific state (0 or 1)

Alarm Suppression / Disablement

The system shall provide the ability to disable or suppress alarms at the following levels:

- For each individual alarm condition
- For all alarm conditions associated with a device or point
- For all alarm conditions associated with an alarm group, process area or displayed on a process graphic

16.5 Minimizing Nuisance Alarms

To minimize the occurrence and effect of nuisance alarms on an operator, the system shall provide the following capabilities for identifying, managing and preventing them.

Alarm Deadbands & Chatter Suppression

To minimize analog input *chattering* (a point going in and out of an alarm condition rapidly) there shall be configurable dead band parameters, on an individual tag basis.

To minimize the occurrence of nuisance alarms during startup / shutdown scenarios the system shall support alarm chatter suppression at the controller level. This feature shall ensure that alarms are not retriggered at the HMI until they have been acknowledged.

HMI Displays for Identifying Nuisance Alarms

To help plant personnel identify nuisance alarms, the system shall provide standard capability to perform and display an alarm frequency analysis which identifies those alarms that have occurred most frequently over a given period of time.

16.6 System Alarm Initiation

Failures of individual components of the system shall result in the generation of an alarm message. A system alarm shall be generated in the event of a failure for the following components at minimum:

- Field device
- Individual I/O channel
- I/O module
- I/O rack
- Communication modules (bus and network)
- Power supplies
- Communication network
- Controller
- Server/clients
- Historical archive server
- Time synchronization

All devices connected to the system communication network shall be monitored for failures. A system alarm shall be generated for each failure detected.

16.7 Process and System Alarms History Retention

All alarms shall be stored in history files with the capability to archive these to removable media. Capability shall be provided to recall these alarms in visible display lists and printed lists according to selectable filtering options.

See also section 23 historical data archives.

16.8 Alarm Annunciation

The system shall be capable of annunciating process and system alarms in ways including but not limited to:

- Activation of an external audible alarm or light
- Activation of the internal PC sound card (playing of .wav files)
- Updating an alarm display with the current alarm
- Updating an alarm overview screen to indicate the occurrence of an alarm in a specific process area / display
- Printing the alarm message on an alarm printer

- Any graphic object associated with the alarm point will change color, shape, appear, disappear, etc. as configured.

Audible Alarm Annunciation

All alarms for a process area may be assigned to any operator station at configuration time. All alarms shall be displayed on the operator station(s) designated. The audible alarm system shall be user configurable for different tones or patterns. A unique tone or pattern shall be capable of being generated based on alarm priority, message class or process area.

The system shall use global alarm acknowledgement allowing a single acknowledgement from any workstation to acknowledge that alarm on all stations and to silence the audible alarm.

Visible Alarm Annunciation

Alarms shall cause visible display annunciation at, and only at, an operator station configured for those alarms. The annunciation shall occur within 3 seconds of detecting the initiating event. It shall be possible to acknowledge process alarms only from an operator station configured for those alarms. It shall be possible for an operator to acknowledge any alarm configured at his station by no more than two actions.

16.9 Alarm Summary Display Lists

The system shall provide the following alarm summary display list capability at a minimum:

- Active Process Alarms
- Cleared Process Alarms
- Acknowledged Process Alarms
- Active System Alarms
- Cleared System Alarms
- Acknowledged System Alarms
- Journal (Alarm History)
- Operator Action List
- Suppressed (Locked) Alarm List
- Shelved (Hidden) Alarm List
- Alarm Frequency Display (Hit) List

Accessing an alarm summary display from any other display shall require no more than one operator action.

Visible display of any alarm shall not clear unless the alarm is acknowledged; and the item initiating the alarm has returned to normal condition.

Multi-page displays may be used. If so, it shall be possible to page forward or backward by a single operator action. The display shall list alarms in tabular format in order of occurrence with the most recent at the top.

It shall be possible to assign alarms to separate areas of the plant so that arriving alarms are entered in area message lists to create an area-related view.

16.10 "Smart" Alarming / Alarm Suppression

To minimize the alarm load on the operator and the presentation of alarms which are meaningless in context, the system shall support "smart" alarming whereby certain alarms can be automatically hidden from the operator based on the occurrence of specific process or plant conditions.

Determination of Plant State or Process Condition

The system shall provide a standard function block for determining / signaling changes in plant state or process condition from within the control strategy. This function block shall be capable of being combined with user-defined logic.

Configuration of Smart Alarming

The system shall provide tools and capability for easy configuration of which alarms will be "hidden" based on plant state or process condition. The configuration interface shall be a standard part of the Engineering system. It shall provide a spreadsheet style interface where alarms can be configured to be hidden / not hidden based on a simple checkbox.

Recording and Display of Hidden Alarms

Hidden alarms shall not be presented to the operator on the standard alarm displays or on process graphics, but their occurrence shall be recorded in the alarm history (journal). A "hidden alarm" display will be provided which lists all of the alarms that are currently hidden from the operator.

16.11 Alarm Shelving

To help plant personnel respond effectively to nuisance alarms or during plant upset conditions (alarm floods), the system shall provide the capability for the operator to manually hide individual alarms or groups of alarms on a temporary basis. A central configurable timer shall monitor how long the alarm has been "on the shelf" and will place it back in the operator's view when the time has elapsed. A comprehensive display listing "hidden alarms" shall be provided to show alarms that have been hidden automatically based on smart Alarm Suppression techniques and manually based on operator shelving.

16.12 Alarm Management and Performance Monitoring

To monitor and optimize the performance of the operator in conjunction with the alarm system, the following capabilities shall be provided by the system as a standard.

Configuration of Troubleshooting information and Corrective Action

The system shall support the configuration of an information text message for each alarm state. This information text message can be used to display the probable cause of an alarm or the recommended corrective action. Information text messages shall be viewable from the standard alarm display list.

Recording of Alarm Comments

The system shall support operator entry of a comment upon acknowledgement of an alarm. The comment shall be stored in the alarm history where it shall be associated with the event. Comments shall be viewable at a later point in time from within the alarm history. To make it easy to locate alarms that have been commented, the alarm history display shall indicate which alarms have received comments and support quick identification by sorting and/or filtering.

Alarm Frequency Displays

To help plant personnel identify nuisance alarms, the system shall provide standard capability to perform and display an alarm frequency analysis which identifies those alarms that have occurred most frequently over a given period of time.

Alarm Message Duration / Time to Acknowledge Displays

To help plant personnel continuously improve operator response to alarms and to minimize the number of standing alarms, the system shall provide a display indicating the amount of time each alarm was active along with the amount of time that elapsed before it was acknowledged.

16.13 Event-Driven Communication

To minimize the communication load on the system bus, change-based communication shall be used by the system for the communication of alarms and events as well as for the communication of process data from the control system to the operator interface.

17 Diagnostics and Troubleshooting

On-line and off-line diagnostics shall be provided to assist in system maintenance and troubleshooting. Diagnostics shall be provided for every major system component and peripheral: including controllers, clients, servers, and communication devices. If diagnostics do not exist for particular peripheral devices such as printers and terminals, the system must detect and provide an error indication for the failure of these devices.

It shall be possible to monitor and troubleshoot PROFIBUS devices and HART devices from the control room without having to go out into the field. The system shall be capable of storing calibration information and device status history for each field device. It shall also be possible for the system to upload field device configuration changes implemented in the field. Once the configuration information is stored in the system, it shall be possible to download it to any other similar device, whether a new or replacement device.

The system shall provide the capability of communication channel problem/error diagnosis.

The Operator Interface shall provide a heartbeat function to monitor the state of all the controllers and HMI components, and generate a message when a change is detected.

If a failure is detected in any backup equipment, the operator shall be notified and the failure shall be logged.

17.1 Events

All events generated by the system shall be captured and logged electronically in a to the event database, in chronological fashion, on a hard disk on one or more servers or single stations.

It shall be possible to retrieve and sort events by time (ascending or descending order) or by type.

All system events shall be time stamped at the point of origin. Events generated in the controller shall be time-stamped in the controller. Those generated in the workstation shall be time stamped in the workstation.

System events shall be defined to include the following at minimum:

- Intelligent Field Device Change in Status (e.g. Fault, Maintenance Required)
- Channel Failure (e.g. Wire Break)
- I/O Module Failure (e.g. Module External Failure detected)
- I/O Rack Failure
- Communication Module Failure
- Power Supply Failure (e.g. Battery Failure, Failure in 24V Source)
- Communication Network Failure (e.g. System Bus Failure)
- Controller Failure (e.g. Failover events)
- Server Failure (e.g. Loss of Redundancy)
- Condition & Performance Monitoring

17.2 System and Diagnostic Displays

On-line displays shall indicate the results of self-diagnostic tests. Failure diagnosis shall be sufficiently specific to indicate which components, modules or devices are at fault. The displays shall be designed to help maintenance and engineering personnel diagnose faults in the system and communications paths. Each category of diagnostic display shall be organized logically to reflect its location in the system hardware architecture.

Within the Operator Interface, a display shall be available showing all controllers and HMI Components with their status.

18 Maintenance and Asset-Management

18.1 Core Functions

The maintenance system shall provide the following core functions:

- Monitoring of the control system components
- Monitoring of technological components (e.g. heat exchangers, valves)
- Monitoring of plant components
- Acquisition of the asset identities
- Condition monitoring
- Acquisition of detail diagnostics
- Interface to specialist tools
- Generation of maintenance requests (including predictive ones)
- Provision of maintenance data for all assets in uniform structure and form for subsequent processing stages
- Commissioning support
- Logging of events and maintenance measures
- Controller load analysis: load, tasks, alarm capabilities when configurable load limits are violated.
- Status of the terminal and system bus redundancy
- Status of inputs/outputs redundancy, channel-based
- Hit list for asset alarms
- Comprehensive asset comments are displayed on the OS
- Up to 10 documents can be assigned to one field instrument
- Performance and load analysis must be possible without additional hardware costs
- The system shall support diagnostics and parameter assignment channel-by-channel.
- Diagnostic information on network (bus load, bursts, data frame loss etc.)

18.2 Required Properties

The maintenance system shall fulfill the following properties:

- Industry sector neutral package
- Integrated in the process control system
- Link to engineering data with no additional configuration or engineering needed.
- Uniform and plant-wide representation of the diagnostics and maintenance state (using uniform symbols or icons).
- Integration of field devices from all manufacturers.
- Separate evaluation of maintenance and process-relevant information.
- Visualization of all plant sections in uniform fashion.
- OS (HMI) "look and feel" in conformity with that of the process system.
- Workflow optimization from diagnostics to completion of the maintenance. It must be possible to minimize production losses and down-time.
- Comprehensive support of condition/state-based maintenance.
- A cyclic export function must be available for storing the diagnostic files for the identification data and device states or device parameters and device states (field device management).

18.3 NAMUR

The system should be based on the following NAMUR recommendations:

- NAMUR NE 91 Requirements for plant oriented Asset Management
- NAMUR NE 105 Requirements for Integration of fieldbus connected instruments in Engineering Tools for Field Devices
- NAMUR NE 107 or VDI/VDE/NAMUR/WIB 2650 Self-test and Diagnostics of Field Devices

The vendor system shall provide component-spanning and automatic system diagnostics & help functions as well as role-based asset processing (read, write, maintenance personnel, specialists).

The system shall provide tools and capabilities which enable preventative and predictive maintenance techniques to be employed for all of the critical assets in a plant including but not limited to motors, pumps, analyzers, transmitters and valve positioners.

18.4 Maintenance System

The maintenance system shall be based on a server / client model. The server can run on dedicated hardware or on the central engineering workstation. Maintenance system clients can be configured on the normal operator interface or on the central engineering workstation.

The server/client system supports the creation of a dedicated and integrated maintenance which can provide comprehensive maintenance information for all plant assets.

The clients configured on the standard HMI shall have the same look and feel as a standard operator HMI displays used for viewing the process.

The basic diagnostic data for all assets will be displayed on a uniform set of faceplates. Detailed diagnostic displays can also be called up representing the following:

- An online view of the hardware configuration
- Online view of a smart field device through the field device management tool

18.5 Integrated Plant Asset Management System

Integrated plant asset management capabilities should be provided by the system for all of the following assets:

- Transmitters & Valve Positioners
- Motors, Pumps and Drives
- Analyzers
- PCs (Servers, clients, historical archives, etc.)
- DCS Hardware (controllers, I/O modules, etc.)
- Networking Equipment (switches, etc.)
- Plant equipment assets (User definable)

The integrated plant asset management shall support the following:

- Configuration and reading of field device parameters via the HART or fieldbus (PROFIBUS-DP/PA, Foundation Fieldbus H1, HART)
- Support a wide range of field devices from vendors allowing additional of new field devices
- Support a common user interface independent of field device vendor
- Support commissioning of devices
- Support device audit trails and change logs
- Support graphic display of device parameters (trend displays, etc.

18.6 Automatic Generation of Asset Management

The system shall automatically populate the asset management database directly from the application program and hardware configuration. No additional entry of basic information for the asset management configuration shall be required.

Faceplates and symbols will be automatically created within the HMI to allow plant personnel to easily visualize and monitor the asset's operating performance. Special summary displays are provided for viewing of asset alarms.

18.7 Condition and Performance Monitoring

It is often necessary to consider certain process, chemical and mechanical conditions in the context of a maintenance concept for a plant. As such the system shall support Condition Monitoring whereby the user can be automatically notified before the operating conditions of critical equipment (such as pumps and bearings) goes beyond acceptable levels.

Standard Function Block for Monitoring of User Defined Assets and Conditions

The system shall provide a standard set of function blocks and faceplates that can be used to monitor the condition and performance of user-defined plant equipment assets. The system shall allow user-defined logic to be combined with the values already measured by the system, in order to monitor the performance of critical assets such as heat exchangers (fouling) and pumps (power consumption, deviations from characteristic curves etc)

The status of user-defined assets shall be displayed within the maintenance station along with those created automatically by the asset management system. Information and status displays will be displayed using a common set of faceplates and summary display lists.

The process automation systems shall provide enhanced performance monitoring and evaluation of pumps and valves in order that preventive maintenance can be performed and the consequences of equipment failure avoided. The performance monitoring will

For pump units, the following functions shall be available:

- Display and analysis of operating performance data (flow, pressure, electrical and mechanical power and efficiency)
- Limit violation of performance valves (mechanical and electrical)
- Overload protection (high flow rate)
- Cavitation or gas conveyance detection
- Blocked rotor and dry-running protection
- Best Operating Point (BOP) and deviation analysis
- Deviations from setpoint analysis
- Pump wear over time
- Statistical data (hours run / stopped)

The functionality shall be available for both fixed and variable speed units.

For control valves, the following functions shall be available:

- Statistical data (maximum hours without motion/hours continuous operation/permitted changes of direction)
- Monitoring of valve response time
- Detection of movement without actuation command
- Displacement of high and low end position

- Determination of remaining control deviation
- Specification of interpolation point coordinates

For flow net components such as pump units, filters, heat exchangers and pipelines the following functionality shall be available:

- Display and analysis of operating performance data (flow, pressure, viscosity, electrical and mechanical power and efficiency) including visualization of:
  - characteristic curves
  - actual operating point
  - pressure drop depending on flow and viscosity

Configuration of advanced performance monitoring shall be via the process automation system engineering station with both manual and self-learning modes.

18.8 Document Management

The system shall include document management capability allowing the storage and display of up to 10 different files (DOC, PDF, MPG, AVI etc.) for each device. This allows information such as standard operating procedures, wiring diagrams, P&IDs or help files, to be called up from the central maintenance station.

19 Batch Processes

19.1 General

The vendor shall provide a batch system with the following functionalities:

- Compliance with S88 Parts 1 and 3
- Designed for DCS, batch and safety applications. It must be able to fulfill high-speed requirements.
- Seamless integration of continuous control, batch control and safety application including uniform software tools.
- It must be possible to use the system in any size plant, scalable from a single-station system up to distributed client-server architecture, for recipe controls in small or large applications.
- Optimally adaptable for all requirements with modular design and flexible scaling.
- Economical realization of recipe-driven batch processes.
- Batch process automation through a batch server and multiple batch clients that work together in a plant project, if required.
- Support for recipe-driven control strategies.
- Simple and flexible handling of tasks with alternating control sequences.
- Easy to use creation of batch names using predefined and dynamic components
- Optional redundant configuration of batch server stations.
- Support for an optional general security system that allows the use of the same user name (logon) and password for both the Microsoft Windows operating system and the batch system.
- The configuration action: download of the batch / operator station configuration must be saved in a log file with a comment.
- The system shall allow changes to the configuration of batch online without interruption to operation.
- The system must provide batch reports with integrated trends views.
- Batch changes in the recipe can only be changed after revoking the release.
- Batch faceplates shall have the same look-and-feel as for the process control system

19.2 Seamless Integration

- The batch system shall be fully integrated in vendor's automation system.
- It must be possible to completely configure the plant data through the engineering system.
- All data required for creating recipes must be forwarded from the engineering system to the Batch server.
- The system shall support separation between recipe editing and the engineering system.
- It must be possible to transfer configuration changes from the engineering system to the Batch server per update function (online/offline).
- The batch system must be able to communicate with the controllers via the vendor's OS.
- It must be possible to integrate operator instructions and dialogs in the communication.
- It must be possible to perform all common configuration tasks (controllers, OS, Batch, and History), the fieldbus configuration (transmitter, drives, analyzers etc.), the database generation and the editing on a single engineering workstation. It must also be possible, however, to use several engineering workstations simultaneously for this work.

19.3 Basic Software Package

The basic package must support at least 10 plant units and offer the following functions:

- The Control Center is the "command center" for monitoring and control of batch processes. It must manage all relevant data via a graphic user interface. Convenient order and batch planning must also be possible along with the graphic display of the unit allocation.
- A monitoring and control center for batch processes
- The Recipe Editor shall be provided for simple, intuitive creation and modification of master recipes and library operations.
- The system shall feature a graphic user interface, typical Microsoft Windows editing function for single and grouped objects as well as a structural syntax testing.
- The recipe creation is based on batch objects from the batch plant configuration by the engineering system e.g. units and technological functions.
- It must be possible to start the Batch Recipe Editor on its own, or from the Control Center.
- It must be possible to easily expand the basic package. Add-on packages must be available for expanding the client-server configuration with additional Batch clients.
- It shall be possible to expand the functions of single stations, Batch clients and Batch servers using add-on packages.

19.4 Optional Add-on Functions

- The system shall enable additional planning functionality through adequate batch planning. Batches must be planned, changed, canceled, deleted and released.
- The system shall support hierarchical recipe structure according to S88
- Recipe procedure for controlling processes or production in plants
- Recipe unit procedure for controlling a process level in plant units
- Recipe operation/recipe function to perform industrial tasks/functions on technical equipment
- The system shall provide a user library for recipe operations. It must be possible to manage and edit it centrally.
- The system shall allow the separation between procedure and formula. The flexibility provided by unit-neutral recipes shall be further increased by separating procedures and parameter sets (formulas).
- It shall be possible to create a variety of master recipes by linking several formulas to a recipe procedure. It must be possible to change procedures centrally.
- It shall be possible to define the structure of the formula with user-defined formula-categories.
- An open interface shall be included for programming special applications for specific branches and projects.
- The import of recipes defined in the description language Batch Markup Language (BATCHML) must be supported.

19.5 Add-ons

- Arithmetic expressions for calculation purposes in phase parameters and transitions.
- Text comparison in transitions
- Versions management: support should be provided for master recipes, recipe operation libraries, recipes with 2 prefix numbers.
- It shall be possible to use product data in recipes.
- Roaming user i.e. user-specific settings can be transferred from one HMI station to another.
- Language interface can be switched directly online
- Integration of route control
- The system shall provide software and hardware redundancy for batch applications
- Recipe related limits can be defined at phase instanances in additional to equipment related limits as well as checking of these limits on operator input.

19.6 Allocation Strategies

The batch system shall support user-defined allocation strategies:

- Process parameters
- Longest unused. The unit longest unused is allocated.
- Operator selection
- Conditions
- Allocation change for an active batch. Tthis shall be possible after the batch start and before the unit allocation.

19.7 Electronic Signature

An electronic signature from the batch system shall be provided for the entire life cycle of a recipe (see also Section 26 Electronic Records / Electronic Signatures) as well as for batch control steps (like start, stop, cancel, delete, comment, etc.). This electronic signature shall be an integrated part of standard system functionality and easily configurable, also containing multiple signature with configurable roles and sequences of signing.

20 Batch (alternative)

For many industries and applications, meeting the requirements and ISA S88 and FDA's 21 CFR Part 11 results in an engineered solution that may not be economical for the application. The following is an alternative requirements specification for batch processes which are less complex and in many cases sufficient.

The process automation system shall provide a standard application frame work for managing the following:

- Materials
  - Materials master data maintenance
  - Material lot data handling and tracking
  - Materials status, consumption, received , stock management
- Parameters (or recipes)
  - Recipe maintenance
- Orders
  - Order lists
  - Oder processing
  - Order status overview
  - Order completion log
- Archives
  - Storage and management of orders, material and recipe data

21 Handling of Material Transports

The quoted DCS shall provide an additional tool for the configuration, control, monitoring and diagnostics of material transports in pipeline networks which is not specialized on any particular industry.

21.1 General

The route control shall provide the following functionalities:

- Operation of range of transport routes from simple to complex
- Automatic route searches for transporting materials in plants and storage depots.
- Configuration, control and monitoring and error diagnostics of material transport in pipeline networks.
- Use in plants with numerous complex route combinations or large storage depots
- Operation of plants with numerous pipelines with high flexibility

21.2 Configuration

The route control configuration shall be based on the basic configuration of the process control system with blocks from the vendor's standard library. It must be possible to simply expand existing plants with the route control.

The system shall offer configuration components:

- Library with uniform interface blocks for configuration
- Wizard as an interface between the route control configuration and process control system basic configuration
- Engineering tool for simple configuration of routes, partial routes and properties

21.3 Architecture

Route control shall be able to use the basic hardware of the process control system.

In small plants, it shall be possible to combine the operator system and route control on a single station.

The route control shall allow client-server configurations, expandable with up to 32 route control clients per server.

It shall be possible to install the control center of the route control on an OS Client or Batch client, but also to configure it as a separate route control client.

The route control engineering must be integrated in the engineering toolset of the vendor's central engineering system.

21.4 Route Control in Runtime

The following runtime components shall be available for operating, visualizing and diagnosing material transports:

- Route control block icons (status of a route, e.g. manual mode, fault etc.)
- Route controls faceplate (operation and visualization for a route)
- Route control center (operation and visualization for all routes)

21.5 Maintenance in the Route Control

Service personnel shall have the option of setting the automation system to the "Maintenance" state for the route control system. New material transports are then blocked.

21.6 Fault-tolerance

The route control system shall support fault-tolerant (fail-safe) and non-fault-tolerant automation systems. Suitable route control library functions must be provided.

21.7 Operating System

The route control system shall run on the Microsoft Windows or Microsoft Windows Server operating systems.

21.8 Engineering Station

The system shall support configuration of the route control servers via the central engineering station. Wizards must be provided for generating the designated communication connections.

21.9 Material Change

The system shall provide the option for manually changing material in an active material transport. It must be possible to set special material properties.

21.10 System Safety Route Control

For system security reasons the system shall allow reading/writing of distributed Microsoft Windows folders only for specific route control user groups. The "everyone" attribute is not allowed.

22 Process Simulation

A process simulator is required to support the following:

- Process and operability analysis to improve plant safety
- Evaluation of abnormal process conditions and equipment failures (pre- and post- event)
- Emergency control and response testing
- Start-up / Shutdown analysis
- Operation procedure optimization
- Operator training (also prior to commissioning)
- Comprehensive equipment testing at factory and controller pre-tuning
- Improve and test operator full graphic displays

The simulator shall:

- be capable of simulating continuously the process. It shall also be possible to simulate field inputs and outputs, field instrumentation and the process automation system.
- be capable to emulate the original controller logic from the plant by using soft PLCs running in a Microsoft Windows environment
- support configuration and download of the controller logic to the emulation by using the actual DCS engineering system. It shall also be possible to use diagnostic functions from actual DCS engineering system.
- support scenario management. It shall be possible to create, save, load, edit and activate scenarios in the simulator.
- provide real time, step through and backtrack modes of operation and it can be stopped and started at any time, providing a virtual time and allow snapshots
- support integration of third-party simulators for complex equipment or processes.
- support different levels of simulation (full, partial, simplified) according to requirements
- allow the firmware update of the connected HW, the modification of names, IP address, subnet masks and the import of GSD and GSDML files.
- support the redundant PROFINET configuration R1 and the Process Alarm PROFINET

The simulator shall fully integrate with the process automation system equipment especially components such as HMI, communication buses, automation components to permit different levels of simulation and provide a near real environment for users.

The simulator shall use the actual plant operator HMI systems and graphic display

The simulator shall work with both virtual process automation system control logic and also with the real controllers. Thus It shall be possible to import existing

architecture information into the system to avoid duplicate data input and the associated error source

The logic and process simulation with the associated emulation shall allow logic validation also referred to as virtual commissioning.

The available know-how of a process engineer or automation engineer should be sufficient for fast, comprehensive training. Special knowledge about simulation should not be necessary.

The simulation system shall be able to run on a PC-based system with Microsoft Windows operating system.

22.1 Controller Simulation

A controller simulation tool shall be available which shall allow simulation of field inputs and outputs within the control logic and to facilitate testing and troubleshooting of the controller program. It shall require no control or I/O hardware and shall be capable of being used to simulate both batch and continuous processes. It shall not require special modifications of the actual controller program to be able to be run in simulation mode.

22.2 Simulation of Remote I/O and PROFIBUS Devices

The system shall support the use of cards which are capable of simulating the actual electrical signals and responses of remote I/O and PROFIBUS field devices to an actual controller.

It must be possible to import the field devices to be simulated, from the hardware configuration of the plant.

The simulation of the PROFIBUS-DP/PA nodes must be performed without reaction by the controller, i.e. the controller shall not distinguish between real and simulated field devices communicating on the bus.

The system shall allow error simulation on the PROFIBUS. This includes:

- Stations failure
- Module failure
- Channel and cable diagnostics

The system must offer simulation of aggregates using prefabricated libraries and editable software functions (sequencers, interlocks, DP redundancy).

The simulation must allow testing of virtual field devices (on the PROFIBUS DP / PA) without mechanical stress or danger to the real installation.

22.3 Process Modeling

The system shall support the use of higher order process simulation programs that are capable of modeling the process dynamics. These programs shall be capable of making use of the actual control program or database extracted from the control program for the development of the model (maximizing reuse), including export / import of the hardware configuration and signal interface data.

The controller simulation shall be able to communicate with various communication interfaces (OPC etc.). The vendor shall provide prefabricated, freely-programmable libraries for this.

The simulation shall allow modeling of process engineering factors with scalable detail precision and support the following functions:

- Drag-and-Drop modeling through a graphic interface
- Integrated mathematics
- Component libraries with definable properties
- Equation-based modeling
- Macro components
- Model sectors
- Dynamic graphics and animations

The system shall allow running realtime simulation. Realtime synchronization must be possible.

It must be possible to save and reuse modeled scenarios. The reuse should be facilitated by integrated management.

The simulation system shall support the connection of process visualization. It must be possible to visualize and animate the simulation.

The system shall support simulation analysis with logs, trends and messages.

It must be possible to test software changes independent of the real plant.

The simulation must run on the process level, device level (actuator/sensor level) and signal level.

23 Historical Data Handling

An integrated historical data management system is required with functional capabilities supporting:

- Capture of process values, alarms, events, and batch data
- Post-processing (average, maximum, minimum, rate of change, data reduction, filtering)
- Archiving
- Retrieval and visualization
- Reporting
- System configuration

The system shall be able to capture data according to a specific project configuration and at the same time respond to any data retrieval requests in a timely manner without impact on data capture performance or degradation.

Users shall be able to access data without specialist process automation system knowledge or supervisors involvement.

The system shall allow selection of any variable in the process automation system to be added and configured for archiving. Variables configured or changed in the process automation system shall be automatically reflected in the historical data management system without additional engineering.

The historical data management system shall comprise two subsystems:

- Short-term subsystem: A local component running on the HMI server to record data from the process control system
- Long-term subsystem: the actual historian, running on a dedicated machine, which collects and archives the data from the short-term subsystem

Both short- and long-term subsystems shall utilize a Microsoft SQL real-time relational database management system (RDBMS) for storage of all process related information.

The short-term subsystem is part of the HMI server and shall provide historical data to clients (HMI, OPC DA client, OPC A&E client, etc.) of the process automation system in the form of:

- Trends
- Alarms and events lists
- Batch data

The short-term subsystem shall be easily configurable and support editing of data to be archived, archive rates, archive types, etc.

The configuration of the short-term subsystem is automatically adopted by the long-term subsystem.

The long-term subsystem shall manage all activities necessary to ensure continued access to archived data for as long as necessary. The long-term subsystem can

interface with higher level systems (such as MES) as well as to other systems requiring process automation system data.

It shall not be possible under any circumstances that users gain data access to the process automation system data network, servers, automation system etc. via the long-term subsystem.

The HMI can display data from both the short- and long-term archive in several forms, such as trends and tables.

23.1 Archiving Capability

The archiving configuration tool shall provide the ability to define archiving rates in increments of, seconds, minutes, hours, or days.

The historian shall include the capability to archive values including but not limited to:

- Actual value
- Maximum
- Minimum
- Sum
- Mean

The historian shall include the capability to archive digital values on either a rising or falling edge.

It shall be possible to associate a unit to archived values.

23.2 Database Capacity

The system shall support archiving of up to 80,000 different variables per HMI Server.

A historical archive server shall support the archiving of up to 140,000 different variables.

At a minimum the historian shall have the capability to continuously archive at least 5.000 values per second.

A data compression algorithm shall be available to minimize the storage space required by the archives.

23.3 Backup/Restore of the Historian Database

The system shall supply tools for backing up the database to removable media or to an alternate storage location. The backup utility must be able to execute the database backups based on either of the following configurable criteria:

- Time-based (e.g. every week)
- The system shall support complete backup of historical data base in one file as well as recovery from it.

23.4 Redundancy

The system shall support the use of redundant historical archives and storage of archive databases on separate servers.

Redundant historical archives will be automatically synchronized when the partner is returned to service.

No Loss of data: If the historian has lost the connection to the HMI server for any reason, the data will be continuously stored on HMI Server (local store-and-forward principle). After the connection is established again, all missing data will automatically be recovered from the HMI Server.

23.5 Third-party connectivity

The system shall support third-party connectivity via:

- OPC UA server
- MQTT cloud connector

24 Trend Displays

Every operator workstation shall provide viewing for real-time and historical trend information. Data collected in any historian package shall be available to all workstations. The system must support a centralized approach to historical data collection.

The system shall support user defined sets of trends so that commonly viewed historical information can be defined in trends once and easily accessed by selecting a pre-configured screen target incorporated in the graphic display. There should be no practical limit to the number of trends that can be defined. Each trend screen shall support up to 8 separate pens. Selection of points to be trended shall be menu driven.

Historical trends shall support seamless integration of both real-time and historical data within a single trend window, with seamless movement between the two. In the event that the screen is scrolled to the left, then historical values will be recalled from historical data files. Scrolling the trend far enough to the right will result in current real-time data being displayed as it is collected.

Zoom in/out and moving forwards and backwards in time shall be possible with no more than two operator actions. A mechanism for selecting a location on the trend, such as a hairline cursor and reading the numeric values of the trends at that point in time shall be provided.

It shall be possible to call up new historic trends and configure them online from the Operator Interface.

Pre-configured real-time trends shall be available from a faceplate.

It shall be possible to export data associated with a currently displayed trend to a .csv file for viewing in MS-Excel.

25 Reporting

The process automation system shall provide an integral reporting subsystem used to report both current and archived data.

The reporting subsystem shall utilize standard tree / list view presentation techniques for management and administration of reports.

The reporting subsystem shall provide the capability to define reports for both visualization and printed format. Report templates shall be supplied which can be modified or used as is.

The reporting subsystem shall allow individual reports to be programmatically modified and/or utilized as part of the Control Logic/Scripting requirements.

The reporting subsystem shall provide the capability to define both the dynamic and static properties reports, including but not limited to:

- Inclusion of archived data, alarm data or event data,
- Customization of the format, layout, and graphical images, included on a report.
- Configuration of automatic report generation, including frequency, destination of the report, and a prioritized list of alternate system resources should problems be encountered during automatic production.

The reporting subsystem shall not impose limits on the number of reports that can be configured.

The system shall support the use of optional third-party applications (i.e. Microsoft Excel, Crystal Reports) for generation of reports.

Report Generation

It shall be possible for all reports to be displayed on a workstation screen as well as printed on a report printer. Hourly, daily, monthly, end-of-month, quarterly and yearly reports shall be supported.

Reports shall be printed and/or saved to disk when a process event occurs. It shall be possible to activate a report in any of the following manners:

- Upon demand (operator request)
- Scheduled (shift, daily and monthly)
- Upon event occurrence

Preconfigured Report Templates

The reporting subsystem shall be supplied with pre-configured reports including but not limited to:

- Graphic display documentation
- Historical archiving
- Alarm archiving

Report exporting

The reporting subsystem shall support exporting of formats in XML and MS HTML formats

26 Electronic Records / Electronic Signatures

26.1 General Requirements

The system shall support access protection and data integrity using:

Access Controls: The system shall limit access to only authorized qualified personnel. The administration of users, user groups and user rights shall be based on central user management.

Data Integrity: The system must provide the ability to record data and to discern altered records. Built-in checks for the correct and secure handling of data should be provided for manually entered data as well as for data being electronically exchanged with other systems.

Record Retention: The system shall have the capability to retain, protect and readily retrieve records throughout the established retention period. Systems must be able to reproduce electronic records in both human readable and electronic form.

26.2 GMP Requirements

In addition to the before mentioned general requirements, the system shall meet the requirements of ISPE GAMP 5, EU GMP guidelines and FDA's 21 CFR Part 11.

Data security and integrity features shall be consistent with controls required by 21 CFR Part 11 to protect electronic records:

Validation: The system shall support lifecycle development documentation adequate to support system validation to ensure precise, reliable and consistent data preparation in accordance with the standards.

Audit Trails: Electronic records shall use secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information.

Electronic Signatures: The system shall provide measures to ensure that utilization of electronic signature is limited to the genuine owner only and that attempted use by others is promptly detected and recorded. Non-biometric systems shall provide two distinct identification components (e.g. user ID and password) to be entered when signing. At least the password must be re-entered for any subsequent signing action within the same session. The system shall include measures to prohibit falsification of electronic signatures using standard tools.

27 Virtualization

The process automation system shall provide the virtualization of OS servers, OS clients and Engineering systems based on VMware ESXi.

The Vendor shall have tested and approved virtualization environment which include virtualization hardware suitable for hosting the guest.

It shall be possible to run several virtualized machines of different types in one suitable sized computer hardware. Calculation guidelines shall enable the sizing of host hardware.

Virtualized machines shall be operable from thin clients running on separate hardware.

Virtualized machines shall be as independent from host hardware as much as possible allowing easy migration to new hardware and protection against obsolescence.

It shall be possible to centrally administer virtualized machines as well as including general maintenance, performing installation, upgrades and backups.

Central monitoring of host system performance shall be possible (operating state, memory load, CPU load, hard disk usage and network loads.

Configuration of real or virtualized OS servers and OS clients shall be transparent to either real or virtualized engineering stations.

The operation of virtualized machines from the operator perspective shall generally be no different to that of real operator clients and servers and any restrictions or limitations shall be clearly identified.

Host machines shall be included in a security concept, i.e. Patches.

28 Advanced Process Controls

The system shall support complex process controls such as:

- Self-tuning / optimization control
- Model predictive control (MPC) with as many as 10x10 manipulated and controlled variables
- Adaptive control (feed forward/backward)
- Virtual sensing (soft sensors or virtual online analyzer) for quantities not directly measurable
- Support external processing with Matlab/Excel
- Fuzzy control

29 Technological Objects

Standardized technologic objects (STO) shall be available for the automation of common typical industrial components and applications. The technological objects shall include:

- Control software object
- Integrated alarm and messaging
- Operator system faceplates for control and monitoring (both for operators clients as well as for local field panels)
- Functional documentation

The purpose of the STO's shall is to reduce the custom application engineering for many standard tasks thus reducing implementation, commissioning and testing time and costs while increasing reliability of the system. The look and feel of the STO's shall be similar to operators

STO's shall be available for:

- Most types of valve (gate, butterfly, check, surge relief, ball and cone, control valves etc.)
- Drives (DOL, star-delta, reversing, dahlander, soft starter, variable speed, positioner,)
- Measured Values (analogue measurements, polygon curve fitting, interpolation, extended limits levels, etc.)
- Heating Ventilation and Air Conditioning modules (thermal outputs, emitted energy, enthalpy, humidity, saturation humidity calculations and conversion functions)
- Schedulers (timers, aggregate switchover, external triggered)
- Mathematical (averaging, filtering, accumulators)
- Permissive hierarchies for distributed applications (multi-level permissive, multi- or parallel control operations, etc.)

30 Links to other Systems & Remote Access

30.1 Support for third-party connectivity

The system shall be capable of communicating with third-party control systems by using of the following interfaces and protocols:

- OPC
- PROFIBUS
- Foundation Fieldbus (FF)
- Ethernet (e.g. Modbus TCP)
- Serial Interface (e.g. Modbus RTU), RK512, 3964R

30.2 Serial Interface

The following capabilities shall be available for communicating to auxiliary systems:

- RS-232C, RS-422, and RS-485 with full and half-duplex operation, and selectable baud rates (19200, 38400, 57600, and 115200)
- IEEE 802.3 Ethernet protocol at 10 or 100 MBPS, with TCP/IP
- Modbus configured in a master-slave relationship, with the system as the master and the auxiliary system as the slave.

30.3 OPC Interface

The system shall be able to communicate bi-directionally with auxiliary systems using OPC. The OPC interface shall be configured in a client-server relationship and as such the system shall be able to act as either the OPC Client or OPC Server as required.

The vendor system shall provide access to alarms and events via OPC standard interfaces DA, HDA, AE, and HAE or OPC UA. OPC UA process tags can be configured as write-protected.

There shall be no need to write any custom code to set up the OPC interface. Configuring the OPC shall be done using drag-and-drop functionality to link the data source and target.

At a minimum, the OPC interface shall support scan rates of 500 ms and 1 second.

The Interface should be capable of handling a Data throughput rate of 10,000 tags / sec.

30.4 Integration with Enterprise Systems

The system shall be capable of interfacing with ERP systems (such as SAP) through the use of optional Information Technology (IT) software modules developed based on the IEC 62264/ISA S95 standards. The following optional IT modules shall be available at a minimum:

- Production Scheduling
- Asset / Maintenance Management
- Material Management
- Historical Records / KPI Management
- Compliance Management

IT Modules shall support a plug-in architecture whereby a Framework is provided for interfacing between the process automation system and the ERP/MES system.

The system shall provide functionality such as "Electronic Batch Log Management" for MES systems.

30.5 Safety with Network Components

The vendor shall ensure maximum security for remote access to ES or controller via LAN. The data traffic between the internal and external network must be controlled by a special network component.

A Virtual Private Network (VPN) Tunnel is required for increased transmission security and transparency.

Encrypted data traffic is required between security modules.

The system network shall offer high performance and standby redundancy. A Gigabit backbone is required. (SCALANCE X414-3E):

30.6 Weighing Systems

The system shall offer integral weighing technology with engineering involving little work.

30.7 Video Integration

The system shall offer video integration.

30.8 Remote Access

It shall be possible to remotely access the system by modem (DSL or ISDN) for troubleshooting purposes.

The user shall have the capability to disable this feature without disconnecting the modem.

31 Electrical Power Systems

The process automation system shall be capable of integrating with electrical power system using the IEC 61850 protocol by means of the Manufacturing Message Protocol (MMS) and Generic Object Oriented Substation Events (GOOSE).

If the electrical power system is based on the FMS/PROFIBUS DP standard it shall be possible to integrate IED's employing this standard.

The system shall be capable of monitoring and controlling the intelligent electronic devices (IED's) of the electrical power system which support the IEC 61850 protocol. Automation of the devices shall be possible but the system is not intended for high speed switching operations.

IED's can be of the types:

- Protection relays
- Electronic sensors
- Power and quality measurements and phase measurement
- Metering systems (revenue or non-revenue)
- Fault recorders

The process automation system shall show interoperability with IDE's from different Vendors.

The process automation system shall have templates for OS clients for the most common IED's. Operators shall be possible to both visualize and control IEC's from the OS Clients.

The OS server shall include any standard firmware, drivers and/or licenses for interface to the IED's using the IEC 61850 protocol. Historical archiving of electrical power information system shall be via standard software requiring only configuration.

An engineering station shall be provided specific for the configuration of the functionality relating to the electrical power system. For the general functions of the electrical power system (e.g. feeder, motor, generator, transformer, line) technological function blocks for the engineering and the visualization (monitoring & operation) should be provided and be integrated homogeneously in the system

The process automation system shall support redundant communications to the IED's. Furthermore the communication system interconnection shall be via fiber optic cable which provides higher EMC immunity in noisy electrical power environments.

Time synchronization is critical with IEC and the process automation system shall be able to synchronize all IED's to within 1 ms.

It shall be possible to automate IED's with an automation system component of the process automation system. The automation system controller shall have all necessary templates and function blocks necessary for connecting to and interfacing with the IED's.

Energy Management

The system shall be able to identify energy-intensive consumers and processes in order to derive Measures for improving the energy efficiency.

The system shall provide load management features to prevent load peaks.

32 Telecontrol

The process automation system shall support integration of remote telemetry terminal units (RTU) via one or more standard telecontrol communication protocols (IEC 60870-5-101, IEC 60870-5-104, DNP3 or Modbus RTU).

Networking Types

Networking of the system control center with the outstations is carried out by means of a WAN (Wide Area Network). The most diverse network types and operating modes shall be supported– including IP-based networks:

- Dedicated lines (copper and fiber optic cables)
- Private wireless networks
- Dial-up networks (analog, ISDN)
- Ethernet wireless
- Industrial Wireless LAN (IWLAN)
- Fiber-optic conductors, e.g. through the use of
- Switches with optical ports
- Mobile services (E)GPRS, or UMTS
- Public or private IP networks (DSL)

The telecontrol system shall have the following characteristics:

- Possible to configure networks flexibly with any combination of topology (star, linear bus, and node topologies)
- Redundant communications
- Support RTU to master station backup communication routes over different communication routes and protocols
- An RTU can interface to multiple master stations simultaneously via different transmission protocols and routes
- Peer-to-peer communication between RTU’s

Telecontrol Application

All data communicated shall be times stamped at origin and RTU's shall support both automatically time synchronization from the process automation system and local GPS time clocks. Switchover between daylight-saving time and standard time shall be automatic where required.

The following data transfer modes shall be possible:

- General interrogation (startup or user initiated)
- Cyclic initiated from master unit
- Spontaneous
- Balanced or unbalanced communication
- Data prioritizing

RTU's shall include all standard functionality for processing of analogue data to reduce telemetry data traffic including hysteresis on absolute and rate of changes values.

The process automation system shall have matching templates at client and server level matching telecontrol specific modules at the RTU level. Templates shall be available for process objects such as motors and valves) as well as for messages and measured values including their corresponding trends.

Remote control and operation shall be configurable to allow compliance with operational safety procedures including remote/local/manual/automatic permissive interlocks. It shall be possible to assign switching authority between different master stations.

Engineering

A uniform engineering platform shall be provided using the engineering system of the process automation system for the configuration of telecontrol components. It shall be possible to configure RTU's and perform maintenance operations from the engineering system if being from the same vendor as the process automation system. RTU's and perform maintenance operations shall be possible without interruption of the RTU.

The process automation shall have standard templates and function blocks which require only configuration for most process objects and it shall be possible to create new user blocks.

Data Security

The telecontrol system shall have comprehensive measures to prevent data corruption and loss.

IP-based networks shall be protected through dedicated VPN solutions and firewalls.

In the event that telecontrol communications are interrupted the RTU shall include local data frame buffer storage technology for continuous recording of data. This will allow missing data to be fully communicated after restoration of communications.

33 Industrial Security

All process control systems should have comprehensive industrial security technical capabilities to prevent unauthorized or unwanted penetration, intentional or unintentional interference with the proper and intended operation, or inappropriate access to information including computers, networks, operating systems, applications and other programmable configurable components of the system.

The system should allow the combination of several possible countermeasures to address industrial security threats, including the following:

- Authentication of users, groups and/or computers
- Access controls
- Digital signatures
- Logging mechanisms
- Scanning for malicious software
- Security patching of software
- Use of whitelisting mechanisms
- System activity monitoring
- Secure remote access
- Physical security

33.1 Use of "Defense in Depth" Architectures

A system holistic approach shall be provided based on different protection layers, so called "defense in depth", described in IEC 62443, such as:

- Plant security
  - Organizational security
  - Physical prevention of access to critical components by unauthorized persons
- Network security
  - Controlled interfaces between involved networks, e.g. with firewalls
  - Allow Network segmentation and security cells
  - Secure communication
- System integrity
  - Malware detection and prevention (e.g. antivirus and whitelisting software)
  - Maintenance and update processes, Patch management
  - Account management (e.g. User authentication for operators
  - Integrated access protection mechanisms in automation components

33.2 Network Architecture

It shall be possible to configure the process automation system according to the concept of zones and conduits as described in IEC 62443-1-1 and FDA 21 CFR Part 11.

The system shall have a range of industrial security products available for the formation of zones and conduits:

- Network modules with integrated firewalls, port filters, NAT/NAPT, DHCP servers, configurable as in router, switch or bridge mode modes, Stateful Inspection, Denial of Service (DoS) protection and bandwidth limiting
- VPN encryption shall be supported
- Encrypted communication on terminal bus shall be default
- IPsec tunnels shall be supported for communication between zones.

The system shall allow clear demarcation between the protected internal network (control system LAN) and unprotected or untrusted external networks. Interfaces, if any, to office IT and the Internet/Intranet are subject to clearly defined security mechanisms - and can be monitored accordingly.

33.3 Securing network access points

Use of Firewalls

The system shall support the use of firewalls to block selective (filter) traffic between network zones (subnets) or from a network to a device. To provide maximum protection, firewalls must allow for rules to be created which allow only necessary access by employing one or more of the following techniques:

- Packet filtering
- IP based rules
- MAC address based rules
- Port based rules
- Stateful inspection
- Network monitoring and logging mechanisms

Supported Firewalls

One of the following firewalls shall be supported as a minimum:

- Microsoft Windows Firewall
- Palo Alto NG
- SIMATIC Scalance SC6x

Security Modules for Industrial Environments

The vendor shall supply rugged, industrial-rated security modules as required, meeting the following characteristics:

- Integrated firewall capable of Filtering on IP-, MAC addresses and ports
- Capable of providing the following additional functions: NAT, DHCP Server, , VPN technology
- Capable of accepting Redundant Power input
- Can be configured / setup without expert security knowledge

Creation of Perimeter Networks - Demilitarized Zones (DMZs)

The system shall support the ability to segment the networks by use of perimeter networks (DMZs). DMZs shall be used to provide a secure access point for the following types of control system connections:

- Data Historian (when it communicates outside the control network)
- Web servers
- OPC servers
- Security servers (e.g. virus scan server management system)
- Microsoft Windows Server Update Services (WSUS)

33.4 User Management and Access Control

Central User Management

The system shall provide the capability of central user/group management within Active Directory (Windows domain) or Windows workgroup providing the following specific capabilities:

- Create, delete, lock-out users
- Create, delete, use of operator rights groups
- Two-level ID (username + password) or Login Device (e.g. Card Reader)

Password Security

To ensure the security of the passwords used for accessing the system, the following capabilities shall be available:

- Specification of password properties (min. length ...)
- Limited time for password validity
- Expired passwords excluded for the next “n” generations
- Forced password change after first Log-On
- Auto – log-off after “n” minutes of inactivity
- Lock-out of users after “n” failed attempts to log-in.

Role-based Access Control (RBAC)

The system shall provide user accounts with configurable access and permissions associated with the defined user role. The system shall support the implementation of the principle of minimal rights whereby users and computers can be configured with the minimum set of access rights necessary to perform their function.

Single Sign On

The system shall provide the ability for Single Sign On (SSO) authentication whereby a single login / password allows a user to have access to all programs (PC / Desktop Access, Engineering Tools, HMI, Batch Management) without requiring re-authentication for each application. The Single Sign on capability shall be capable of being used with Role-based Access Control (RBAC)

33.5 Software Security Patch Management & Testing

The Vendor of the process automation system shall provide demonstrable life cycle security support services for the process automation system including:

- Tests and provisioning of patches/updates for automation system related firmware and automation system application programs
- Tests of security patches/updates for operating systems, Internet Explorer, MS SQL server, MS Office and virus scanners
- Guidance on the installation of patches and performing of updates
- Project internal support for patch/update distribution via a central patch server (e.g. WSUS) in DMZ

Comprehensive public available configuration documentation of security aspects of used automation system components is mandatory.

Continuous and immediate testing of new software security patches is critical to maintaining a secure network infrastructure.

Testing of Microsoft Security Patches

To ensure that the latest Microsoft Security patches have been tested for compatibility with the system, the vendor shall test new Microsoft security patches immediately upon their release. Results of the testing shall be communicated to end users so that they can choose when / if to update.

Windows Server Update Services

The system shall support the use of the Windows Server Update Services (WSUS) from Microsoft as a means to implement effective deployment of security patches on all PCs connected to the process control network. The WSUS Server shall allow viewing of all available updates so that they can be released as required in a procedure determined by the end user.

33.6 Use of Virus Scanners & Malware Detection

The system shall support the installation of Virus Scanners on all PCs attached to the process control network. Recommended Virus Scanner:

- Microsoft Defender Antivirus

Minimizing Impact on System Performance

To ensure that virus scanners do not have a negative impact on system performance, the vendor shall provide guidance on malware detection settings for use with their system based on the results of system compatibility testing.

Updates and Testing of New Signature Files

To ensure that virus scanners are able to be continuously updated to prevent new malware threats, the vendor demonstrable shall test new virus signature files immediately upon their release.

Installation and Operation of Virus Scanners

The Installation and Operation of Virus Scanners shall comply with the following:

- Engineering Stations and all other PCs where engineered data can be introduced to the Control System Network: Virus scanners shall be operated in a real-time mode with continuous scanning of all incoming traffic and shall support manual and periodic scans while offline (Runtime and Engineering)
- Operator Stations: Virus scanners shall be operated in real-time mode with continuous scanning of all incoming traffic (Runtime)

33.7 Auto Configuration of System Security Settings

To increase the default security and to minimize the chance of error during the configuration of security settings, the system shall support the automatic configuration of local Microsoft Windows firewalls, DCOM settings and registry entries.

33.8 Securing Access for Remote Maintenance / Troubleshooting

The system shall allow a secure connection for remote maintenance and troubleshooting. The access point shall be capable of providing firewall technology and as minimum one of the following access and authorization methods:

- Authentication and Encryption with IP Security (IPsec)
- Authentication and Encryption with Secure Sockets Layer (ssl and https)
- Use of VPN (Virtual Private Network) tunneling
- Network Access Quarantine Control for Secure Support Access

33.9 Testing for Security Vulnerabilities

The system shall support the testing for vulnerabilities using the Microsoft Baseline Security Analyzer (MBSA) . Testing shall be able to identify the following conditions at a minimum:

- User accounts without password
- Missing Microsoft security patches

33.10 Security Certification

The process control system shall be Achilles™ certified.

The vendor shall supply a list of components certified to Achilles Level 2.

A security certification according to IEC-62443 shall be demonstrated for the process control system.

34 Safety

Shutdown Systems are deemed safety critical systems and the system functionality must be designed in accordance with IEC 61508 and IEC 61511 to protect people, the environment and assets. The process automation systems shall be suitable to meet appropriate safety integrity levels (SIL) to SIL 3.

Optional fail-safe control operation up to SIL 3 shall be available using standard controller hardware and special fail-safe I/O modules, using simplex and/or redundant configurations. The system shall be modular allowing the system to be configured to meet SIL 2 or 3 requirements Safety Integrated Functions (SIF).

Fail safe systems shall be integrated with (or separate and independent to)[9] the process automation system.

Programming of fail-safe applications shall use the same engineering environment as configuration of process applications and be supported easy to configure cause and effect safety matrices in the controller and HMI.

The safety related functionality shall be met with the system having the highest availability due to an architecture with multiple fault tolerance capability and integrated safety fieldbus.

Safety critical applications (SIL 1 to 3) will be performed by a logic solver compliant with IEC 61508 and certified by an independent body (TÜV or equivalent).

The safety system shall be integrated with (or part of)[9] the process automation system. All visualization of safety functionality will be via the process automation system.

The application logic shall be protected against unauthorized modification or access by from external sources.

Configuration of Safety Systems

The configuration of fail-safe systems shall automatically supplement user-specific CFCs with functions required for error detection and reaction. The configuration of fail-safe systems shall be performed with the same tools used for the non-fail-safe application.

The system shall support safety programming with:

- CFC according to IEC 61131-3
- Cause-and-effect safety matrix for programming

Configuration of safety functions shall be via using a safety matrix that automatically generates safety-related CFC charts. The automatically generated safety blocks shall comply with SIL 3 requirements.

A standard tool shall be available for calculations to ensure that each safety loop meets the availability and reliability required by the allocated SIL rating. Failure rates for each safety system component of each loop as documented shall be input into each SIL calculation.

[9] Depending on project objectives and requirements

Support for Safety Communication

The system shall support the use of PROFIsafe for communication to and from smart instruments even in a redundant / fault tolerant architecture. The PROFIsafe protocol ensures that reliable and fail-safe communication (up to SIL 3) takes place between smart field devices and their controller over PROFIBUS PA.

34.1 Optional Library for Fail-safe Controllers

The system shall support the optional addition of a specific library of fail-safe function blocks. These function blocks must be certified by technical inspectorate and easy to distinguish from those used for non-fail-safe applications. It must be possible to link and configure the blocks with the CFC tool:

Use of Shared Hardware

To minimize spare parts requirements the system shall support shared use of hardware (CPU, power supply, backplane bus and communication modules) for both safety-related and non-safety-related applications.

35 Explosion Protection

The vendor shall offer future-proof distributed solutions for automation system in hazardous areas. It should be possible to integrate these solutions quickly and easily in every controller via the system bus.

35.1 Distributed Hardware

The system shall provide intrinsically safe interfaces / couplers and distributed I/O and additional I/O's which are intrinsically safe and can be configured for safety critical applications to SIL Level 2 and 3 (see Section 34).

Capability for use in Zones 2 and 1 is a requirement. It should also be possible to operate actuators and sensors in Zones 0/20. It shall be possible to install process I/O directly in Zone 1 areas. It should be possible to also use the I/O Interfaces and couplers in hazardous areas (Ex areas).

They should be designed modular and flexible and satisfy rugged design norms.

It should be easy to perform the installation using rails and integrated connectors.

It should be possible to connect the sensors and actuators via the bus system.

Permanent wiring shall be possible, to make it easier to exchange modules without removing the wiring. It should be possible to perform replacement during ongoing operation (hot swapping). It should be possible to hot swap interfaces in the Ex area.

All devices are certified according to the ATEX Directive 94/9/EC.

35.2 Configuration and Diagnostics

The configuration and diagnostic capability shall be available locally or centrally via the configuration of the vendor system.

Full online expandability shall be possible.

35.3 Hardware Specification and Limits:

The vendor system shall offer distributed solutions providing at least 3 of the requirements listed below.

Requirement 1 also fulfills requirements 2 and 3

Requirement 2 also fulfills requirement 3

	Requirement 1	Requirement 2	Requirement 3
ATEX 94/9/EC IEC 60079-0	II 2 G (1) GD EEx de [ia/ib] IIC/IIB T4	II 3 G EEx nA II T4/T5	II 3 G EEx nA II T4/T5
FM NEC 500 / 505	IS, Class I Zone 1 EEx ib [ia] IIC, T4 Class I, II, III Division 2 Groups A, B, C, D, E, F, G, T4	Class I Division 2 Groups A, B, C, D, T4/T5 Class I Zone 2 IIC, T4/T5	Class I Division 2 Groups A, B, C, D, T4/T5 Class I Zone 2 IIC, T4/T5
Temperature 2	–20º C to +70º C	0º C to +60º C	0º C to +60º C

36 Equipment Installation

As per projects required – to be developed by user.

37 Documentation

Documentation covering the system hardware, software, and configuration tools shall be available.

The system vendor shall provide a complete set of CDROM/DVD based manuals.

The system shall offer comprehensive context sensitive help.

Whenever possible, the vendor shall supply custom documentation by using standard functionality embedded in the system. All documentation shall be provided in English, German, French, Italian, Spanish and Portuguese.

A plant documentation utility shall be available, which generates plant documentation in accordance with standards.

38 Support Services

The vendor shall offer phone and email support, Internet information, and training courses.

The vendor shall offer global 24/7 support for all system hardware and software. This shall include spare parts, maintenance, and technical support.

The vendor shall offer a published 800 number for telephone support during normal business hours.

Telephone support related to current product issues shall be free of charge during business hours

The vendor shall offer comprehensive self-directed technical support via the Internet that shall include but not be limited to:

- Contact with technical support via email
- Searchable knowledge base
- Product catalogs and manuals
- Product Frequently Asked Questions (FAQs)
- Synchronized system software update collections
- Application examples
- Application Tips

As an option the vendor shall offer a comprehensive software maintenance plan that shall include but not be limited to providing:

- Latest product version(s)
- Updated knowledge base
- Updated electronic manuals

39 Training

The vendor shall offer complete and comprehensive training programs for operators, engineers, commissioning and maintenance personnel as well as for Information Technology & Networking specialists. The training shall cover the basic process automation system as well as for specialist equipment and applications covered in the specification.

The vendor shall be able to offer bespoke training programs and provide a structured standard published training program which personnel can attend.

39.1 Basic Process Automation System Training

The basic training shall cover the following equipment:.

- Controller hardware training course content shall include, but not be limited to:
  - - CPU, power supply, communication cards, backplane, local and remote I/O racks.
  - - I/O cards
  - - PROFIBUS-, PROFINET and Ethernet communication
  - - Fault tolerant architecture and fail-safe architecture.
- OS training course content shall include, but not be limited to:
  - - OS system overview
  - - OS client and server architecture, including networking and redundancy
  - - The display hierarchy, and the graphical, trending, alarm, reporting, and batch displays
- Controller engineering training course content shall include, but not be limited to tools for:
  - - Configuration of the I/O hardware devices
  - - Configuration of the communication networks
  - - Configuration of continuous and sequential control operations
  - - Design of operating and monitoring strategies
- OS engineering training course content shall include, but not be limited to tools for:
  - - Creation of an OS system application
  - - Administration and management of OS system database
  - - Creation, administration and management of graphics displays
  - - Administration and management of system alarming
  - - Administration, and management of the historical subsystem
  - - Administration, and management of the reporting subsystem
- Maintenance training
- System administrator training

39.2 Advanced Training

A modular advanced training shall be available corresponding to the requirements of this specification covering specialist hardware and application software:

Example:

- Advanced process control
- Technological objects
- Telecontrol
- Batch or routing systems
- Electrical power systems
- Asset management
- Process functional safety

40 References

Equipment supplied to this specification shall comply with the following standards as detailed in the requirements of this document:

- **International Electrotechnical Commission (IEC)[10]**

IEC 60079-0:2011-06 Explosive atmospheres - Part 0: Equipment – General requirements

IEC 60079-10-1:2015-09 Explosive atmospheres - Part 10-1: Classification of areas - Explosive gas atmospheres

IEC 60079-10-2:2015-01 Explosive atmospheres - Part 10-2: Classification of areas - Combustible dust atmospheres

IEC 60529 Ed. 2.1:2009-10 Degrees of protection provided by enclosures (IP code)

IEC 60751:1983-01 Industrial platinum resistance thermometer sensors

IEC 60870-5-101:2003-02 Telecontrol equipment and systems - Part 5-101: Transmission protocols; Companion standard for basic telecontrol tasks

IEC 60870-5-104:2006-06 Telecontrol equipment and systems - Part 5-104: Transmission protocols - Network access for IEC 60870-5-101 using standard transport profiles

IEC 61000-6-2:2005 Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity for industrial environments

IEC 61000-6-4 Ed. 2.1:2011-2 Electromagnetic compatibility (EMC) - Part 6-4: Generic standards - Emission standard for industrial environments

IEC 61131-2:2007-07 Programmable controllers – Part 2: Equipment requirements and tests

IEC 61131-3:2013-02-01 Programmable controllers - Part 3: Programming languages

IEC 61158-1 Ed 1.0:2014-05 Industrial communication networks – Fieldbus specifications - Part 1: Overview and guidance for the IEC 61158 and IEC 61784 series

IEC 61158-2:2014-07 Fieldbus standard for use in industrial control systems - Part 2: Physical Layer specification and service definition.

IEC 61508-1:2010-04 Functional safety of electrical/ electronic/ programmable electronic safety-related systems - Part 1: General requirements

IEC 61508-2:2010-04 Functional safety of electrical/ electronic/ programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

IEC 61508-3:2010-04 Functional safety of electrical/ electronic/ programmable electronic safety-related systems - Part 3: Software requirements

[10] IEC standards are referenced - for European projects/supply equivalent EU Harmonized Standards should be selected if available.

IEC 61508-4:2010-04 Functional safety of electrical/ electronic/ programmable electronic safety-related systems - Part 4: Definitions and abbreviations

IEC 61511-1:2016-02 Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and software requirements

IEC 61511-2:2016-07 Functional safety - Safety instrumented systems for the process industry sector - Part 2: Guidelines for the application of IEC 61511-1

IEC 61511-3:2016-07 Functional safety - Safety instrumented systems for the process industry sector - Part 3: Guidance for the determination of the required safety integrity levels

IEC 61784-1 Ed 3.0:2010-07 Industrial communication networks – Profiles - Part 1: Fieldbus profiles

IEC 61804-2:2006-09 Function blocks (FB) for process control - Part 2: Specification of FB concept

IEC 61804-4:2015 Function blocks (FB) for process control and electronic device description language (EDDL) - Part 4: EDD interpretation

IEC 61850-8-1:2011-06 Communication networks and systems for power utility automation - Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3

IEC 62061 Ed.1.2:2015-08 Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems

IEC 62443 Industrial communication networks – Network and system security

IEC 62443-2-1:2010-11 Industrial communication networks - network and system security - Part 2-1: Establishing an industrial automation and control system security program

IEC 624433-3-3: Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels

IEC 624433-4-1: IT-Security for Industrial Automation Systems - Part 4-1: Secure Product Development Lifecycle Requirements

IEC/TR 62541:2010-02 OPC Unified Architecture

IEC 62682:2014-07 (draft) Management alarms for the process industry

- **Institute of Electrical and Electronics Engineers (IEEE)**

IEEE Std. 1815:2012 for Electric Power Systems Communications - Distributed Network Protocol (DNP3)

IEEE 754:2008-01 Floating-point arithmetic / date of publication

IEEE 802.3XX Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications (series)

- **Object Linking and Embedding for Process Control (OPC) Foundation**

Standards as per www.openfoundation.org and referenced in this specification preceded with OPC.

- **The OPC Unified Architecture (UA)**

OPC UA is a platform-independent, service-oriented architecture that integrates all functionalities of the individual OPC Classic specifications into an extensible framework.

- **National Fire Protection Association**

NFPA 70 Article 250 (Applicable version valid at location) also known as National Electrical Code – Grounding and Bonding

NFPA 70 Article 500 (Applicable version valid at location) also known as National Electrical Code – Hazardous (Classified) Locations, Classes I, II, AND III, Divisions I AND 2

NFPA 70 Article 505 (Applicable version valid at location) also known as National Electrical Code – Zone 0, 1 and 2 locations

NFPA 79 (2007) (Applicable version valid at location) NFPA 79 Electrical Standard for Industrial Machinery

- **National Electrical Manufacturers Association (NEMA)**

NEMA 250:2008-01 Enclosures for Electrical Equipment (1000 Volts maximum)

- **Underwriters Laboratories**

UL Certificate

- **Canadian Standards Association**

CSA Certificate

- **International Organization for Standardization (ISO)**

ISO 9001:2015-09 Quality management systems – Requirements

ISO 11064-5:2008-07 Ergonomic design of control centres - Part 5:Displays and controls

ISO 13849-1:2006-11 Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design

ISO 10418:2003-10 Petroleum and natural gas industries - Offshore production installations - Analysis, design, installation and testing of basic surface process safety systems

- **International Society of Automation** (ISA)

ISA/ANSI 84.00.01:2004-09 Functional safety of safety instrumented systems for the process industry sector - Part 1 Framework, Definitions, System, Hardware and Software Requirements

ISA/ANSI 84.00.02:2004-09 Functional Safety: Safety Instrumented Systems for the Process Industry Sector — Part 2: Guidelines for the Application of ANSI/ISA 84.00.01 2004 Part 1 (IEC 61511-1 Mod) Hardware and Software Requirements

ISA/ANSI 84.00.03:2004-09 Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 3: Guidance for the Determination of the Required Safety Integrity Levels - Informative

ANSI/ISA 88.00.0X Batch Control Part 1: Models and Terminology; Part 3: General and Site Recipe Models and Representation; Part 4: Batch Production Records (referred to as ISA S88 in this document)

ANSI/ISA 95.00.0X Enterprise-Control System Integration Parts 1-5

- **European Commission**

Conformité Européenne (CE) manufacturer's declaration that the product meets the requirements of the applicable EC directives:

- Equipment for potentially explosive atmospheres (ATEX) Directive 2014/34/EU
- Electromagnetic Compatibility (EMC) Directive 2014/30/EU
- Low Voltage Directive (LVD) 2014/35/EU
- Machinery Directive (MD) 2006/42/EC

EU Guidelines to Good Manufacturing Practice, Volume 4, Annex 11; (2011)

- **US Government**

US Food and Drug Administration (FDA) 21 CFR Part 11[11] – Electronic records: Electronic signatures (ERES)

- **International Society for Pharmaceutical Engineering (ISPE)**

Good Automated Manufacturing Practice (GAMP). GAMP 5 A Risk-Based Approach to Compliant GxP[12] Computerized Systems

- **EEMUA**

EEMUA 201 Ed.2:2010 Process plant control desks utilizing human-computer interfaces: a guide to design, operational and human-computer interface issues

- **NAMUR**

NAMUR NE 91 Requirements for plant oriented Asset Management

NAMUR NE 105 Requirements for Integration of fieldbus connected instruments in engineering Tools for Field Devices

NAMUR NE 107 or VDI/VDE/NAMUR/WIB 2650 Self-test and Diagnostics of Field Devices

- **Other**

Modbus RTU:2002-12 MODBUS over serial line specification and implementation guide V1.0 (Modbus Org)

[11] CFR = Code of Federal Regulations published by the government of the United States.

[12] GxP is a general term for Good (Anything...) Practice

41 Definitions

This section contains definitions for acronyms, abbreviations, words, and terms as they are used in this document.

41.1 Acronyms and Abbreviations

CAD	Computer Aided Design
CAE	Computer Aided Engineering
CFC	Continuous Function Chart
CPU	Central Processing Unit
DCS	Distributed Control System
DHCP	Dynamic Host Configuration Protocol
DOL	Direct Online
DMZ	Demilitarized Zones
ECC	Error-Correcting Code memory
EDDL	Electronic Device Description Language (IEC 61804)
EIA	Electronic Industries Association
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ERP	Enterprise Resource Planning
ES	Engineering Station
FDI	Field Device Integration
GPS	Global Positioning System
HART	Highway Addressable Remote Transducer
HMI	Human Machine Interface
HTML	Hyper Text Markup Language
I/O	Input/Output
IEC	International Electrotechnical Commission
IL	Instruction List
IPsec	Internet Protocol Security
ISA	The Instrumentation, Systems, and Automation Society
ITP	Industrial Twisted Pair
MAC	Media Access Control address
MES	Manufacturing Execution Systems
MQTT	Message Queue Telemetry Transport Protocol
MTA	Marshalled Termination Assembly

MTBF	Mean Time Between Failures
NAT	Network Address Translation
NAPT	Network Address & Port Translation
OLE	Object Linking and Embedding
OPC	OLE for Process Control
OPC UA	OPC Unified Architecture
OS	Operator Station
PC	Personal Computer (X86-64 or x64 based computer architecture)
P&ID	Process and Instrument Drawing
PID	Proportional Integral Derivative
PG	Panzergewinde (German:Stahlpanzerrohrgewinde standard for screw threads - DIN 40430)
PO	Process Object
PSU	Power Supply Unit
RAID	Redundant Array Independent Disks
RFI	Radio Frequency Interference
R-LAD	Relay Ladder Logic
RIO	Remote Input/Output
RTD	Resistance Temperature Detector
RTX	Real time extension for Microsoft Windows
ROP	
SFC	Sequential Function Charts
SIF	Safety Integrated Function
SIL	Safety Integrity Level
SQL	Structured Query Language
ST	Structured Text
STO	Standardized Technological Object
TCP/IP	Transmission Control Protocol / Internet Protocol
VSD	Variable Speed Drive
VPN	Virtual Private Networks
WLAN	Wireless Lan
XML	Extensible Markup Language

Telemetry

DSL	Digital Subscriber Link

FMS/PROFIBUS DP Fieldbus Message of PROFIBUS Decentralized Peripherals

GOOSE	Generic Object Oriented Substation Events (IEC 61850-8-1)

GPRS	General Packet Radio Service	
GPS	Global Positioning System	
IED	Intelligent electronic device (IEC/TR 61850-1)	
IP	Internet Protocol	
ISDN	Integrated Services Digital Network	
IWLAN	Interworking Wireless LAN	
MMS	Manufacturing Message Protocol (ISO 8802-3)	
PSTN	Public Switched Telephone Network	
RTU	Remote Telemetry Unit	
UMTS	Universal Mobile Telecommunications SystemWAN	Wide Area Network

41.2 Words and Terms

Alarm Logging: Editor for configuring the message system in the operator station and the application for displaying, archiving, and handling messages.

Archive: Saving measured values and messages in the operator station to history so the data can be called up over a long period of time.

AS-Interface: The Actuator Sensor Interface is a networking system for field mounted binary sensors and actuators.

Audible signal device: Horn, bell, buzzer, or similar device indicating that a new alarm or message has arrived at the operator station.

Availability: The probability that a system will be able to perform its designated function when required.

Blocks: Blocks are separate parts of a user control software configuration distinguished by their function, structure, and purpose.

Bus: A path for electrical signals allowing the exchange of data between various components of a computer or system.

Central Processing Unit (CPU): The central part of the controller in which the user program is stored and processed, and the operating system and communication interfaces are contained.

CFC: Continuous Function Chart is a high-level graphical language using function blocks for configuring continuous control systems.

FDI (Field Device Integration)**:** A technology that allows a uniform device integration for all control systems, field devices and protocols

GSD (General Station Description): Communication features of a Profibus device are always described in a GSD file.

GSDML (General Station Description Markup Language): The functionality of a Profinet IO field device is always described in a GSD file.

MRP (Media Redundancy Protocol): With the MRP, a redundant PROFINET communication without switches can be implemented via a ring topology.

Chart: The document in which the automation functions can be created using the CFC tool or the SFC tool.

Conduit: Logical grouping of communication assets that protects the security of the channels it contains

Communications Link: The hardware and software that performs the transmitting and receiving of digital information over a communication system, for example a bus.

Configurable: The capability to select and connect standard hardware modules (blocks) to create a system; or the capability to change functionality or sizing of software functions by changing parameters without having to modify or regenerate software.

Configuration: The physical installation of hardware modules to satisfy system requirements; or the selection of software options to satisfy system requirements.

CSV: Comma Separated Values, an ASCII text format in which tabular data are saved.

Cycle: In the controller, the scanning of inputs, execution of algorithms by the controller, and transmission of output values to devices.

Cybersecurity: Actions required to preclude unauthorized use of, denial of service to, modifications to, disclosure of, loss of revenue from, or destruction of critical systems or informational assets

DCF77: Long wave time signal and standard-frequency radio station provided by the Physikalisch-Technische Bundesanstalt (PTB)

Discrete Control: Control where inputs, algorithms, and outputs are based on logical (True or False) values.

Distributed I/O: Field devices or analog and digital modules located at a distance from their central controller.

Engineering Workstation (ES): Computer equipment that includes a PC, a monitor, a keyboard and an appropriate pointing device, used by technically-trained personnel to configure the control system.

Ethernet: Hardware type standard for data transmission using coax, twisted pair, fiber optic cable, or wireless, usually running at 10 Mbps (see Fast Ethernet).

Faceplate: On the Operator Station screen, a graphic element that represents, for example, an analog controller instrument, a hardwired push-button, or a switch, allowing operator monitoring and control of the device.

Fast Ethernet: A faster version of Ethernet running at 100 Mbps. (IEEE 802.3u-1995)

Fault-tolerant system: A system in which all essential components (such as CPU, Power supplies, racks etc.) are duplicated, allowing the backup device to take over from the primary device without control interruption if a failure occurs.

Foundation Fieldbus: The ISA/IEC Foundation Fieldbus standard covers a communication system for field mounted measurement and control devices. (IEC 61784 and IEC 61158)

Function Block Diagrams (FBD): A control bock as defined in IEC 61131-3. Also FB or Block.

Gigabit Ethernet: Ethernet with transmission rates of 1000 Mbps

GPS: Global Positioning System, a satellite based system, which provides the exact position anywhere on earth and the time of day.

Human Machine Interface (HMI): The graphical interface program for allowing an operator to interact with and control a process.

Instance: A copy of a function block, which is used again in the control configuration for a similar application.

Instruction List (IL): Instruction List is a textual programming language resembling machine code and complying with IEC 61131-3.

Invalid Value: The state of a tag value, which indicates that the quantity being measured or calculated, is out-of-range, not measurable, or not calculable.

Ladder Diagram (LD): Graphical representation of the automation task using relay symbols complying with IEC 61131-3.

Lifebeat Monitoring: An operator station program, which monitors the controllers, servers, and operator stations, and provides a plant picture with the status.

Logs: Files or printouts of information in chronological order.

Mode: Control block operational condition, such as manual, automatic, or cascade.

Module: An assembly of interconnected components that constitute an identifiable device, instrument, or piece of equipment. A module can be disconnected, removed as a unit, and replaced with a spare. It has definable performance characteristics that permit it to be tested as a unit.

OPC: Object Linking and Embedding for Process Control, a software application, which allows bi-directional data flow between two separate applications.

Operator Station (OS): Electronic equipment on which the HMI resides, including, at a minimum, PC workstation, a monitor, keyboard, and pointing device used by an operator to monitor and control his assigned process or manufacturing units.

R1 System Redundancy: a modular PROFINET device with redundant communication interface builds more than one communication link to a redundant controller.

S2 System Redundancy: A PROFINET device with a communication interface builds more than one communication link to a redundant controller.

PLC: Programmable Logic Controller, used for discrete and continuous control in processing and manufacturing plants.

PROFIBUS: Process Fieldbus, a fieldbus complying with EN 50170 Vol. 2 PROFIBUS (DIN 19245; bus system for industrial application based on PROFIBUS).

Plug and Play: The ability of hardware equipment to automatically identify itself to the system. When the equipment is powered up it is automatically assigned a unique identity without the need to set any dipswitches.

Point: A process variable derived from an input signal or calculated in a process calculation.

Process Object: A collection of variables and parameters that performs a control function (e.g. motor, block valve, PID Controller) which may consist of more than one I/O point.

Redundant: A system/subsystem with two modules that provides automatic switchover to a backup in the event of a failure, without loss of a system function.

Regulatory Control: The functions of process measurement, control algorithm execution, and final control device actuator that provide closed loop control of a plant process.

Reliability: The probability that the system or component will perform its intended function for a specified period of time, usually measured as Mean Time Between Failures.

Structured Text (ST): A high-level language complying with IEC 61131-3 and resembling Pascal for programming complex or custom logic tasks within the controller.

Self-Diagnostic: The capability of an electronic device to monitor its own status and indicate faults that occur within itself.

Security: System access control by key lock, password, electronic card, or other equivalent method.

Sequential Control: A type of discrete control handling sequential processes.

Sequential Function Chart (SFC): Sequential Function Charts are a high-level graphical configuration language for sequential control applications.

System Bus: The network used for communication between controllers and HMI servers.

Tag: A collection of attributes that specify either a control loop or a process variable, or a measured input, or a calculated value, or some combination of these, and all associated control and output algorithms. Each tag is unique.

Tag Id: The unique alphanumeric code assigned to inputs, outputs, equipment items, and control blocks. The tag ID might include the plant area identifier.

Terminal Bus: The network used for communication between HMI Clients and HMI servers.

Time synchronization: Time Synch is provided by the operator station to make sure that all PLCs and operator stations on the bus operate with the same time of day.

Virtualization: Virtualization refers to the runnable mapping of one or several computers on a real computer.

Zone: Grouping of logical or physical assets that share common security requirements

42 Trademarks

Microsoft®, Windows®, Windows Server®, Windows 7®, Internet Explorer®, SQL Server®, Excel®, Access®, ActiveX®, Visual Basic® are either registered trademarks or trademarks of Microsoft Corporation

OLE, DCO, COM are technologies developed by Microsoft that allow embedding and linking of objects.

Adobe®, PostScript® and Acrobat® are registered trademarks of Adobe Systems, Incorporated.

BATCHML was specified by the World Batch Forum (WBF).

AutoCAD® is a registered trademark of Autodesk, Incorporated.

X Window System is a trademark of The Open Group

SAP®, Sybase®, Crystal Reports® are the trademarks or registered trademarks of SAP AG in Germany and in several other countries or an SAP affiliate company

HTML, XML, are trademarks, registered trademarks, or claimed as generic terms by the Massachusetts Institute of Technology (MIT), European Research Consortium for Informatics and Mathematics (ERCIM), or Keio University on behalf of W3C World Wide Web Consortium

PROFIBUS is a trademark of the PROFIBUS User Organization.

HART® is a registered trademark of the HART Communication Foundation.

McAfee, Virusscan® are registered trademarks of McAfee Inc.

OfficeScan® is a trademark or registered trademarks of Trend Micro Incorporated

Symantec AntiVirus™, Norton® is a trademark or registered trademarks of Symantec Corporation or its affiliate

Foundation™ Fieldbus is a trademark of the Fieldbus Foundation

GAMP® is a registered trademark of the International Society for Pharmaceutical Engineering

TÜV® is the trade mark for the TÜV organizations and the non-profit Association of TÜVs (VdTÜV).

Achilles™ is a registered trademark of Wurldtech Security Inc. in Canada and/or other countries.