Totally Integrated Power

Process Control Systems (DCS)

Process Control System SIMATIC PCS 7

TEXT	SIMATIC PCS 7 (Control System)
TEXT	SIMATIC PCS 7 for powerrate
TEXT	Maintenance Station

Specification
for a
Process Automation System

Contents

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, auxiliary systems, and management information systems. All field instrumentation used with the process control system must meet the minimum applicable requirements set forth by the International Electrotechnical Commission (IEC) standards listed below.

2 References

Equipment supplied to this specification shall comply with the latest edition of the references listed below, unless otherwise noted.

- **International Electrotechnical Commission (IEC)**

  IEC 60751 (1983-01) Industrial platinum resistance thermometer sensors

  IEC 61000-4-2 (2001-04) Electromagnetic compatibility (EMC) - Part 4-2: Testing and measurement techniques - Electrostatic discharge immunity test.

  IEC 61000-4-3 (2002-03) Electromagnetic compatibility (EMC) - Part 4-3

  IEC 61000-4-4 (1995-01) Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques - Electrical fast transient/burst immunity test.

  IEC 61158 (2000-08) Fieldbus standard for use in industrial control systems - Part 2: Physical Layer specification and service definition.

  IEC 61131-3 (1993-03) Programmable controllers - Part 3: Programming languages

  IEC 61508: Functional Safety, Safety Related Systems

- **National Fire Protection Association**

  NFPA 70 National Electrical Code

- **Underwriters Laboratories**

  UL Certificate

- **Canadian Standards Association**

  CSA Certificate

- **ISO-9001**

  The supplier's quality management system fulfills all the specifications of the ISO 9001 standard.

- **GMA-NAMUR**

  The system fulfills the requirements specified by the GMA-NAMUR committee on validation.

  NA= NAMUR Worksheet (Arbeitsblatt)

  NE= NAMUR Recommendation (Empfehlung)

- **CENELEC / ATEX**
- Guideline 94/9/EG for Explosion Protection
- **NEC (National Electrical Code) Standard 500**

- **ISA/ANSI**

  S88.01 – Batch Control Part 1: Models and Terminology

- **DIN 40 050 / IEC 529 / VDE 0470/ EN 60529**

  Defines Degrees of Protection

3 General

3.1 For All Applications

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

The system should provide a client-server architecture.

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

The system must be designed for DCS, safety and PLC 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 field bus devices from any manufacturer without additional certification.

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

The vendor system must support separation between the terminal and system bus. Connection to an office bus may not lead to a problem.

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

3.2 DCS, PLC, Batch and Safety System Combination

The process automation system shall include features traditionally associated with both a programmable logic controller (such as programming in ladder logic, and remote I/O architectures) and a distributed control system (such as continuous and complex control, advanced operator interfaces, sophisticated redundancy). 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.

3.3 Horizontal Integration

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

3.4 Vertical Integration

The system shall support vertical integration by utilizing uniform data communication structures to support complete integration from the ERP, MES, control and field levels.

3.5 Open System

The system shall be an open system composed of standards-based technology including PC platforms with a Windows operating system, Ethernet communications, TCP/IP, OPC for interconnectivity of multiple systems from different suppliers, field mountable control system, remote IO subsystem, and bus-based serial communication with field devices over PROFIBUS-DP/PA, Foundation Fieldbus H1, HART, AS-I, and Modbus networks.

The system software is resistant to third-party programs. It must be possible to install all system components. The use of virus scanners must be possible.

3.6 Decentralized Architecture

The system shall have a decentralized client/server architecture allowing extensive scalability. The system shall be expandable and support up to 10 engineering workstations, 32 operator displays – where each station has access to the entire plant, twelve redundant servers, and 60,000 process tags.

3.7 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.

3.8 Fail-safe Controllers

Optional fail-safe control operation shall be available using standard controller hardware and special fail-safe I/O modules, using simplex and/or redundant configurations. Programming of fail-safe applications shall use the same engineering environment as configuration of process applications.

The system shall support modules with high degrees of protection (for example, IP6x).

3.9 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.

Written Explanation of Licensing Practices

To help minimize risk associated with changes in project scope, if software is licensed on a tag-by-tag basis the vendor shall supply in writing details on how the required software license would change under the following circumstances:

- If the total number of system I/O was increased
- Modifications to the set-up of I/O modules (e.g. converting 20% of the discrete inputs into analog inputs. This only applies when the vendor cannot fulfill the demands mentioned in chapter 3.9. It in no way implies dilution of the requirements described there.
- If the user would like to pass real-time variables from his system to a 3rd party OPC Client.

Smart 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 OS and controller in the application.

The engineering system must control and count the POs.

3.10 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. The vendor's standard system operating software shall not be modified to meet any of the user's requirements.

Application software shall be designed in a manner that requires no modification to the system operating software.

Software design shall be such that future revisions or updates of the system operating software will not affect the successful operation of the system.

The vendor must offer the same platform for safety and non-safety applications.

3.11 Spare Capacity and Expansion

Each system shall be supplied with 10% 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 ten percent (10%) 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. There shall be no cost penalty for expansion.

3.12 Software Revision

Application software shall not require modifications in order to be able to run under new releases of the system operating software. Any new release of system software shall be backward compatible with files created using the previous software releases. When a new release is installed, it must be possible to back up the user data since the manufacturer may change the data with the new release.

3.13 Solutions for Small DCS

The vendor must offer a PC-based DCS with hardware CPU for special application areas.

The vendor must offer a PC-based DCS with software CPU and RTX operating system for special application areas.

The vendor must offer a PC-based DCS with hardware CPU for lab automation applications.

4 Environmental Conditions

4.1 Indoor Installations

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

- Temperature range: 0 degrees C to 60 degrees C.
- Relative humidity: 5% to 95% RH.

4.2 Outdoor Environment

It shall be possible to install the I/O system in outdoor enclosures in Class 1 Div 2 (Groups A, B, C, and D) and CENELEC/ATEX Zone 2 hazardous environments.

4.3 Storage Environment

It shall be possible to store the equipment before installation for up to 6 months in an air-conditioned building under the following conditions:

- The equipment shall be packed in a moisture proof container
- Storage temperature: -40 to 70 degrees C
- Relative humidity (outside the moisture proof container): 5% to 95%.

5 Electrical Requirements

5.1 Electrical Area Classification

Buildings containing the control equipment will be rated as electrically unclassified.

5.2 Electromagnetic Compatibility (CE Compliance)

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

5.3 Wiring and Cabling

PROFIBUS, 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.

It should be possible to use safe connectors without short-circuit and the risk of missing connection.

5.4 Cabinet and Workstation Grounding

AC Safety ground and instrumentation circuit ground shall conform to the NEC, Article 250.

5.5 Circuit Boards

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

6 Controller

6.1 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 msec., required for programmable logic control, and slower processing times required for process control, shall both be available. A minimum of 6 independent scan rates should be available for optimizing the execution time of the application program.

6.2 Large Capacity Controller

The vendor shall provide a large capacity controller capable of executing a minimum of 1000 standard PID Control loops with a 500 msec. scan 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:

Execution time: 18ns

Memory: 30 MB

A firmware update must be possible for redundant systems during ongoing operation.

The vendor shall offer a controller in the upper performance range for more than 750 I/Os.

No connected engineering system containing required data in the controller must be necessary for a cold restart.

The vendor system shall not encounter high CPU load or memory requirements for saved texts in the controller. The variable length texts are to be stored in a text database.

6.3 Controller Redundancy

For high reliability applications, optional redundant controllers, power supplies, Ethernet connections, racks, and Profibus networks shall be available.

Physical Separation of Redundant Controllers

To minimize the potential for common cause failures, redundant controllers shall be able to be physically separated (not located in a common backplane) by up to 10,000 m (32,000 feet). It is not permissible to share a common backplane.

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 msec or less including all I/Os and including no loss of alarms or messages.

Connected redundant I/O components must switchover within 30ms if a fault occurs.

6.4 Power Requirements

Power Supply

There shall be a choice of a 24 VDC or 115/230 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 restart where it left off upon power restoration.

Response to Power Failures

In the event of an extended power failure the controller shall not require access to the engineering station to reload or redo any portion of its configuration.

The system must ensure that programs are not deleted if power fails. This should be ensured with battery backup.

6.5 Choice of Configuration Languages

Configuration languages shall be offered that are traditionally associated with both a DCS and a PLC programming environment. These shall include the following six programming languages including those described in standard IEC 61131:

- Continuous Function Charts (CFC)
- Sequential Function Charts (SFC)
- Structured Control Language (SCL)
- Relay Ladder Logic (R-LAD)

- Instruction List (STL)
- Function Block Diagram
- Safety Matrix (for Safety System Configuration)

6.6 Closed-loop-control

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

6.7 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.

6.8 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 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:

- Proportional Integral Derivative (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 scan rates as fast as 100 times per second (10 ms) shall be possible.

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.

6.9 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.).

6.10 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.

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 ISA S88.01 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

6.11 Supervisory Control

The vendor shall be able to supply standard supervisory control functions fully integrated with the regulatory control 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.

6.12 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“ (similar to Microsoft Excel®) to assist engineers and technicians who are unfamiliar with the tool.

6.13 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 can not 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.

.

6.14 Variable Scan Rates of Control Functions

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

The minimum scan rate for discrete and analog control functions shall be 10 msec.

6.15 Cabinets

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

The standard cabinet shall conform to IP40, and a cabinet upgrade to IP55 shall be available.

The controller and I/O modules shall not require the use of cooling fans.

The vendor must offer switches suitable for mounting in switchgear cabinets.

6.16 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 a minimum of 100 Mbps 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 cable (Industrial Twisted Pair) 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.

6.17 Reserve CPU Capacity

To reserve CPU capacity for future growth and insure rapid software response to process upsets, CPU execution of the configured software application shall not exceed 50 percent CPU time during the course of normal process monitoring and control.

7 Inputs and Outputs

7.1 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.

Analog input and output modules shall provide pass through capability to exchange non-control data, both PROFIBUS 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.

7.2 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)

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 (up to 6.0 miles / 9.6 km with copper cable or longer distance when fiber-optics are used) from their associated controller.

7.3 Non-proprietary Communication from Controller to I/O

Open standards should be used to communicate between a controller and its I/O modules to facilitate connectivity of 3rd 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 (Fieldbus communication).

7.4 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.

The system should offer optimal integration of redundant Remote I/O racks (RIOs), redundant I/Os and field bus (Profibus PA and DP), 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.

7.5 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, and ±1 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

7.6 Digital Inputs

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

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

7.7 Analog Outputs

The system shall support output types of 0-20 mA, 4-20 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

7.8 Digital Outputs

The following solid state output ratings shall be available:

- 24 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.

7.9 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.

7.10 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 scan rates of 10 ms.

7.11 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 individual blown-fuse indication and redundant power connections. A common MTA shall support connection to a redundant or non-redundant I/O configuration.

8 Fieldbus Integration

8.1 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 3rd Party Devices

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

8.2 High Speed Fieldbus Segment (H2) / PROFIBUS DP

High density H2 field bus segments

The H2 segment (PROFIBUS DP) 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 H2 Segments per Master

The system shall support up to 8 PROFIBUS DP (H2) 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 motors and drives via PROFIBUS DP without requiring the use of gateways or interposing PLCs.

8.3 Process Automation Fieldbus Segment (H1) / PROFIBUS PA

Communication rates with process field devices connected to the H1 field bus 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 field bus.

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 H1 segment from the field all the way back to the vicinity of the controller.

Number of Devices per H1 Segment

The H1 field bus 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 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 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 H1 field bus segment shall include built-in intrinsically-safe barriers to connect these types of devices.

8.4 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 the H1 level for PROFIBUS PA.

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

Field Device Distribution Box

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 4 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

Online Configurability

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

8.5 Process Automation Fieldbus Segment (H1) / Foundation Fieldbus (FF)

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

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"

8.6 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.

8.7 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.

9 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) shall be accessible via an integrated configuration tool.

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

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.

9.1 Supported Architectures

The system shall support the following networking topologies for setup of the System Bus: Linear, Tree, Ring, Star, and Redundant.

The system shall support the following networking topologies for setup of the Terminal Bus: Linear or Redundant.

9.2 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 msec or less
- Fanless design
- Extended temperature range - 0 degrees C to 55 degrees C

9.3 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.

9.4 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.

9.5 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.

10 System Configuration - General

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 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 messages to/from Excel and Access 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 MS 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 CAx 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 charts 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, SYBASE, X Window 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
- Field bus 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
- Implementation of the FDA requirements (Food and Drug Administration)
- Process object view with test mode
- Data communication with a CAx 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 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 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 (Deep 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, Spanish, Italian and French 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.

11 Configuration of Control Strategy

11.1 Choice of Configuration Languages

Configuration languages shall be offered that are traditionally associated with both a PLC and DCS programming environment. These shall include the following programming languages including those described in standard IEC 61131:

- Continuous Function Charts (CFC)
- Sequential Function Charts (SFC)
- Structured Control Language (SCL)
- Relay Ladder Logic (LAD)
- Instruction List (STL)
- Function Block Diagram (FBD)
- Safety Matrix (for programming of Safety Systems)

11.2 Continuous Function Chart

A continuous function chart (CFC) tool conforming to IEC 61131-3, shall be available for graphical configuration and connection of function blocks. The CFC tool positions, parameterizes, and connects predefined function blocks using an auto routing and integral message configuring function.

It shall be possible to embed a CFC inside another CFC for creation of unit- or equipment-control applications.

It shall be possible to embed CFC charts to a nesting depth of eight. (Support from macro functions)

Connections between function blocks shall require no more than two mouse clicks no matter where they are located, by using auto routing. The auto routing function shall prevent wiring from falling on top of each other.

The tool shall support comprehensive syntax checking during configuration.

Double clicking a connection shall turn the wiring a different color and shall open the destination of the connection, for example, another CFC chart or the I/O module where the signal is connected.

The system shall support trend displays of up to 8 trends in the CFC. It must be possible to export the displayed values.

The vendor system shall enable drag-and-drop across charts in the CFC with tracking of the interconnections.

11.3 Sequential Function Chart (SFC)

A sequential function chart (SFC) tool shall be available for graphical configuration of sequential and batch processes per IEC 61131-3. Steps and transitions shall be graphically configured using a convenient editing function. The tool shall support comprehensive syntax checking during configuration.

Connections to continuous control functions shall be available using simple actions such as *Browse*, *Drag and drop* and *Fill in the blanks*.

The operator’s visualization display shall be automatically created, including dynamic step/transition boxes, overview, navigation display, and list boxes.

To minimize configuration time, the system shall automatically connect SFC steps and transitions during configuration, based on their placement in the SFC chart, without requiring the user to manually connect them.

The SFC tool shall provide a standard interface for configuration of the three phases of execution of a step (Initialization, Execution and Termination).

The vendor system must be able to display multiple SFC groups with their current states in a picture in tabular form.

11.4 Structured Control Language

A structured control language (SCL) shall be available which utilizes a high-level text-based language whose global language definition conforms to IEC 61131-3. This language, which is similar to PASCAL, shall be capable of being used to program calculations, complex optimization algorithms, define HMI attributes / behavior and to call other function blocks directly from within the program. It shall support the use of a subroutine style of programming to maximize modularity and reuse. Function Blocks created using SCL can be used throughout the program like standard function blocks in the CFC Editor.

11.5 Ladder Logic

The system shall support programming in Ladder Logic using syntax similar to a relay ladder logic circuit diagram. The elements of a circuit diagram can include normally open contacts, normally closed contacts, function blocks etc which can be combined to form networks per IEC 61131-3.

11.6 Instruction List

The system shall support the use of a Statement List Programming Language (STL) which utilizes a structure similar to machine code. Each statement shall represent a program processing operation of the CPU. Multiple statements shall be capable of being linked to form networks IEC 61131-3.

11.7 Function Block

The system shall support configuration using function blocks according to IEC 61131-3.

The user shall be able to modify the appearance and behavior of function blocks by simple modification of an object's property sheet.

Function blocks shall have integrated startup characteristics which govern their behavior during cold start, warm start and hot start conditions.

11.8 Safety Matrix

The system shall support the configuration of Safety System programs using a cause and effect matrix, which allows the user to easily relate process events (inputs or causes) to shutdown devices (outputs or effects) by listing all possible causes on one axis and all effects on the other. The relation of causes to effects is defined by marking the appropriate box (intersection) in the matrix. Configuration of matrix should be simple and intuitive by employing familiar Windows point and click, drag and drop, and dialog box style editing.

11.9 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 that a user can create and download is only limited by the memory capacity of the target controller.

11.10 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).

11.11 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.

11.12 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 create a *Dynamic Display List to* view and manipulate selected real-time input and output values from the control strategy 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. [TBR Fritz – does PCS 7 have this capability]

11.13 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 MS Windows Explorer-like interface to graphically highlight what elements of a configuration are different (CFCs, SFCs, Function Block types, Scan Rate Order 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.

Read/Edit Protection of Function Blocks

The system shall support the locking of user-created custom function blocks. This ensures that the contents of the custom block cannot be viewed or edited, allowing users such as OEMs to securely protect their intellectual property.

11.14 Integrated FDA Functionalities

The vendor shall offer wide-ranging FDA functionalities in his system, including features listed in the following:

- System Logon
- User administration and access control
- Staged permission levels

- Change log: recording of all changes during the production
- Automation system : program download, changes in test mode for CFC/SFC, download of hardware and communication configuration
- OS: program download
- Batch and route control: program download
- Change log: changes in projects and libraries, logons/logoffs, opening and closing projects and libraries, changes to settings
- Version management (version trail): versioning of projects, libraries, multi-projects, recipes
- Comparing/updating projects (Version Cross Manager): CFC/SFC, hardware configuration, communication configuration, OS alarms, plant hierarchy, SFC details (step, transitions, properties etc.)

11.15 General

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

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.

11.16 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 and Foundation Fieldbus H1.

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 3rd 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 field bus instruments.

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

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.

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 field bus 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

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 3rd 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.

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 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 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
- Maximum desktop size of 1600 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, Windows Meta File WMF, and Enhanced Windows Meta File EMF), status displays, text lists, 3D bars, buttons, check boxes, radio boxes, and sliders.

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 (operator station).

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 with MS Excel and Visual Basic.

13.8 Automatic Creation of Display Navigation

A hierarchical navigation scheme (similar to folders in Windows Explorer) 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
- Visual Basic Script (VBS)
- Visual Basic for Applications (VBA)

The programming environment shall support the following functions:

- Ability to access properties and methods of all Active-X controls included with the application or provided by a 3rd 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®.

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 12 servers or 12 redundant pairs of servers. Each server or pair of servers shall be able to communicate with up to 32 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 Central Archive Server.

In general it should be possible to add a redundant OS Server or Central Archive Server to a non redundant structure at any time.

All clients shall have complete visibility to all servers and the central 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 Windows operating system, and industrial Ethernet communications.

The system shall support the Window operating systems Windows 2000/XP/2003.

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

14.3 Monitors

Monitors for operator stations shall be as follows or better:

- Diagonal measurement 21 inches nominal
- 1280 x 1024 resolution
- 32,000 colors

14.4 Multi Monitor operation

The system shall support quad graphics cards with a resolution of up to 1600x1200 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 msec 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 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 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 50 web clients simultaneously.

HMI Web Client

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

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 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.

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 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.

15.6 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, French, Spanish, Italian and German shall be supported at a minimum. Re-programming, recompilation, or reconfiguration of the HMI software application shall not be necessary to achieve this functionality.

15.7 Security

The system must permit following virus scanners compatible to MS Windows on the real-time computers:

- Trend Micro "Office Scan" Corporate Edition V7.3
- Symantec AntiVirus Corporate Edition V9.0 (Norton Antivirus)
- McAfee VirusScan Enterprise V8.0 (only together with patch 11 (KB43256) from McAfee)

The system security shall be modeled after Windows XP but configurable in a manner appropriate for control operations.

The system security configuration tool shall provide an easy to use, simple interface, which offers full support for standard 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 system security 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 Windows operating system, the engineering environment, the HMI and for the Batch system.

15.8 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 the Microsoft operating system.

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)

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.

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
- Central 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.

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 Hiding

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 / Manual Alarm Hiding

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 provided to show alarms that have been hidden automatically based on smart alarm hiding 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.

17 Industrial / Cyber Security

In order to protect the process automation system from the danger of hacker attacks, viruses etc., the vendor / system shall provide comprehensive industrial / cyber security capabilities consisting of products and procedures (best practices).

17.1 Use of "Defense in Depth" Architectures

The system shall support the use of a "Defense in Depth" strategy as recommended by the US Dept of Homeland Security. "Defense in Depth" advocates the creation of a nested security architecture by division of the plant into secure and closed security cells / segments with clearly defined and monitored access points.

17.2 Rules for Creation of Security Cells and Segments

The following rules shall be followed to ensure the creation of secure and fully functional security cells and segments:

- Each segment must form a self-sufficient "zone" that can be operated for a certain amount of time without connection to other segments; thus a segment must be capable of operating autonomously for a period of time.
- All components contained in a segment and involved in its function should be connected to one another (not through leased lines)
- Units that cause high network and computer load when connected from the outside via a complex security mechanism should be integrated directly in the segment
- Access to a security cell should take place only after the user's identity has been verified and logged and only under supervision of authorized persons, for example, physical access by operators.
- All connections to the Control System LAN should be routed through a firewall, with no connections circumventing it.

17.3 Securing network access points

The system shall allow clear demarcation between the protected internal network (control system LAN) and unprotected or untrusted external networks.

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
- Circuit level gateways
- Proxy gateways
- Stateful inspection

Supported Firewalls

The following firewalls shall be supported at a minimum:

- Windows XP Personal Firewall
- Microsoft ISA Server 2004

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, Data encryption
- IP 30 Protection
- Operating Temperature Range: 0℃ to +60℃
- Capable of accepting Redundant Power input
- Can be configured / setup without expert security knowledge

Creation of Demilitarized Zones (DMZ)

The system shall support the ability to segment the network by use of demilitarized zones (DMZ). 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
- Security servers
- SUS Servers

17.4 User Management and Access Control

Central User Management

The system shall provide the capability of the central management of users within domains or workgroups providing the following specific capabilities:

- Create, delete, lock-out users
- Ensure IDs are unique
- 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 for 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)

17.5 Software Security Patch Management & Testing

Continuous and immediate testing of new software security patches is critical to maintaining a secure network infrastructure.

Support for Immediate Installation of Microsoft Security Patches

If deemed necessary by the user, it shall be permissible to load the following new MS Security Patches on the system as soon as they are released from Microsoft:

- Windows operating system
- Internet Explorer
- SQL Server

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.

Software Update Service

The system shall support the use of the Windows Software Update Service (SUS) from Microsoft as a means to quickly and effectively implement automatic deployment of software updates and security patches on all PCs connected to the control network. The SUS Server shall allow viewing of all available updates so that they can be released as required in a procedure determined by the end user.

17.6 Use of Virus Scanners & Malware Detection

The system shall support the installation of Virus Scanners on all PCs attached to the control network. The following Virus Scanners shall be supported at minimum:

- Trend Micro Office Scan
- Symantec Norton Antivirus
- McAfee Virusscan

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 shall test new virus signature files immediately upon their release. Results of the testing shall be communicated to end users so that they can choose when / if to update.

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)

17.7 Auto Configuration of System Security Settings

To minimize the chance of error during the configuration of security settings, the system shall support the automatic configuration of Windows firewalls and registry entries.

17.8 Securing Access for Remote Maintenance / Troubleshooting

The system shall be capable of providing a secure connection for remote maintenance and troubleshooting. This access point shall be securable through use of local firewalls and virus scanning software at a minimum. The following methods shall be supported:

- Authentication and Encryption with IP Security (IPsec)
- Authentication and Encryption with Secure Sockets Layer (ssl and https)
- Use of VPN (Virtual Private Network) tunneling and Network Access Quarantine Control for Secure Support Access

17.9 Testing for Security Vulnerabilities

The system shall support the end user or designate testing for vulnerabilities using the Microsoft Baseline Security Analyzer (MBSA) or equivalent. Testing shall be able to identify the following conditions at a minimum:

- Open ports and protocols in use
- Missing Microsoft security patches

18 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.

18.1 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

18.2 Smart Event Suppression

The system shall provide smart event suppression whereby only the highest order error is reported to the Operator Interface. For example failure of an entire I/O Rack will result in the presentation of an I/O Rack error message, but not in an error message for each individual module located in the rack or from each individual channel of each module.

18.3 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.

18.4 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 Historian (Archive) database
- Adding a new Control Loop to the Configuration

19 Maintenance and Asset-Management

19.1 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.)

19.2 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.

19.3 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.

19.4 Maintenance Station

The system shall support the creation of a dedicated and integrated maintenance station which can provide comprehensive maintenance information for all plant assets.

It shall provide the same HMI interface (look and feel) as a standard operator HMI display that would be 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

19.5 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
- PC's (Servers, Clients, Historians, etc.)
- DCS Hardware (controllers, I/O modules, etc.)
- Networking Equipment (switches, etc.)
- Plant equipment assets (User definable)

19.6 Auto Generation of Asset Management Database & Visualization

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.

19.7 Integration of Smart Motor Control Centers (MCC)

The system shall support the direct integration of Smart Motor Control centers via PROFIBUS. This will allow information on the motor's operating condition to be sent directly to the system via a digital field bus. Optional pre-engineered libraries of function blocks and faceplates shall be available to support easy integration of Smart MCCs into the controller and HMI applications.

19.8 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.

19.9 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.

20 Batch Processes

20.1 General

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

- Compliance with ISA Norm S88. 01 and 03
- 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.
- 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 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.

20.2 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 field bus 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.

20.3 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 centre 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.

20.4 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 ISA S88.01:
  - 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.

20.5 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, ROP 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 (OS) to another.
- Language interface can be switched directly online
- Integration of route control
- The system shall provide software and hardware redundancy for batch applications.

20.6 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 (this shall be possible after the batch start and before the unit allocation).

20.7 Electronic Signature

An electronic signature from the Batch system shall be provided for the entire life cycle of a recipe.

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 vendor's 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 Windows XP Professional or Windows 2003 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 Windows folders only for specific route control user groups. The "everyone" attribute is not allowed.

22 Process Simulation

The system shall support various levels of tools for simulation of processes.

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

The system shall allow commissioning in a virtual plant.

The system shall support training for plant personnel.

It shall be possible to import existing architecture information into the system to avoid duplicate data input and the associated error source.

A fully graphic user interface should simplify operation. 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.

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 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 and signal level.

23 Historical Data Handling

The Operator Interface shall provide a complete historical (archiving) subsystem providing the user the capability to capture and analyze historical data.

A high-performance central archive server shall be provided for handling (long-term) archives. The system shall allow selection of any point in the system to be added and configured for archiving.

The archiving system shall utilize a Microsoft SQL real-time relational database for storage of all process related data. Flat file or internal proprietary databases will not be accepted.

The archiving system shall be configured using standard tools provided by the system to facilitate the display and editing of archive rates, archive types, etc. from graphical and tabular data displays.

The system shall support the online addition of new tags to the historical database with out interrupting operations.

The historical subsystem shall promote the visualization of historical data in both tabular and graphical form. This includes the capability to view historical data via a web-enabled interface.

23.1 Archiving Capability

The historical subsystem shall provide the ability to define archiving rates in increments of milliseconds, seconds, minutes, hours, or days.

The historical system shall allow an individual archive rate to be programmatically modified and/or utilized as part of the Control Logic/Scripting requirements specified above.

The historical subsystem shall include the capability to archive values per analog point including but not limited to:

- actual value
- maximum
- minimum
- sum
- mean

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

23.2 Database Capacity

The system shall support archiving of up to 10,000 different variables per OS Server.

A central archive server shall support the archiving of up to 150,000 different variables.

At a minimum the historical subsystem shall have the capability to continuously archive at least 1000 samples of up to forty (40) data values at any rate from 500 ms to one hour.

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

23.3 Backing Up the Database

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

- Time-based (e.g. every 24 hours)
- Based on the size of the database (e.g. after the size reaches 1 MB)

23.4 Redundancy

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

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

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 Operator Interface shall provide an integral reporting subsystem used to report both current and archived data.

The reporting subsystem shall utilize standard Windows 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. 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

26 Reliability

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.

26.1 Redundancy

Redundancy shall be available over all levels of the automation system, including controllers, power supplies, networks, I/O racks, Clients, and HMI servers, Batch servers and Historians.

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 twelve 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 checkpoint data missing data to the previously failed server. This operation shall occur in the background, and shall not effect the operation of the on-line server.

Flexible, modular redundancy is cost-effective, since it is only used where it is needed.

- Each component can be configured redundantly (2-3 fold redundancy). If required, up to SIL3 (1oo1, 1oo2, 2oo3) and spatial separation shall be possible.
- Redundant field bus architecture allows multiple errors without causing interruption. A ring-shaped field bus 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.

27 Safety

The vendor of the process control system shall offer integrated control and safety functions that provide the following advantages:

Control and Safety functions are integrated in the vendor system, meaning less hardware is required, less personnel training is necessary and the system is easier to operate.

Highest availability due to architecture with multiple fault tolerance

Highest flexibility since safety and standard application is possible in a single CPU and PROFIsafe can be used simultaneously on PROFIBUS.

Integrated safety field bus.

Less wiring, prepared for safe process instrumentation.

Safe life cycle engineering with safety matrix.

No additional communication busses needed for fail-safe technology.

No additional controller needed for fail-safe technology.

The system shall support safety programming with CFC and other fail-safe tools.

27.1 Support of Safety Systems

Execution of Safety Programs

The controller shall support the optional execution of safety programs up to SIL 3, according to IEC 61508.

27.2 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.

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.

27.3 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.

28 Remote Access and Links to other Systems

28.1 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
- Serial Interface (e.g. Modbus), RK512, 3964R

28.2 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.

28.3 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. 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.

28.4 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 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

28.5 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.

28.6 Safety with Network Components

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

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):

28.7 Weighing Systems

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

28.8 Video Integration

The system shall offer video integration.

28.9 High-Performance Controller (closed-loop) Hardware

The system must support the optional integration of high-performance closed-loop controller hardware.

29 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.

29.1 Distributed Hardware

The system shall provide intrinsically safe interfaces / couplers for the distributed I/O, field devices.

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.

It should be possible to hot swap interfaces in the Ex area.

“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 also use the I/O Interfaces and couplers in hazardous areas. (Ex areas)

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.

All devices are certified according to guideline 94/9/EC.

The system shall be compatible for universal I/O cards, to avoid high storage costs.

29.2 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.

29.3 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
CENELEC	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	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
Temperatur2	–20º C to +70º C	0º C to +60º C	0º C to +60º C

30 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 and French.

A plant documentation utility shall be available, which generates plant documentation in accordance with standards.

31 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)
- Software updates
- 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

Training Programs

The vendor shall offer complete and comprehensive training programs for the system, including the controller, networks, and OS.

- 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 and Ethernet communication
  - Fault tolerant architecture and fail-safe architecture.
- OS hardware 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:
  - Introduction to Windows
  - Creation of an OS system application
  - Creation, administration and management of OS system database
  - Creation, administration, and management of graphics displays
  - Creation, administration, and management of system alarming
  - Creation, administration, and management of the historical subsystem
  - Creation, administration, and management of the reporting subsystem
  - HMI Scripting

The vendor shall offer regularly scheduled classes at training centers in all areas/regions of the country. The vendor shall publish course schedules and allow customer registration via the Internet.

32 Definitions

This section contains definitions for acronyms, abbreviations, words, and terms as they are used in this document.

32.1 Acronyms and Abbreviations

AGLP	Add Domain User Account to Global Group, Add Global Group to Local Group and Assign Permission
ALP	Add User Account to Local Group and Assign Permission
CPU	Central Processing Unit
EIA	Electronic Industries Association
EMI	Electromagnetic Interference
HART	Highway Addressable Remote Transducer
HMI	Human Machine Interface
IEC	International Electrotechnical Commission
I/O	Input/Output
ISA	The Instrumentation, Systems, and Automation Society
MTBF	Mean Time Between Failures
OLE	Object Linking and Embedding
OPC	OLE for Process Control
OS	Operator Station
PC	Personal Computer
PO	Process Object
RFI	Radio Frequency Interference
RTX	Real time extension for Windows

32.2 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.

Chart: The document in which the automation functions can be created using the CFC tool or the SFC tool.

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.

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.

Gigabit Ethernet: Ethernet with transmission rates of 1000 Mbps

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.

Function Block: A control bock as defined in IEC 1131-3. See also Block.

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.

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 logic (LAD): Graphical representation of the automation task using relay symbols complying with DIN 19239.

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.

PLC: Programmable Logic Controller, used for discrete and continuous control in processing and manufacturing plants.

PROFIBUS: Process Field Bus, a field bus 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 Control Language (SCL): A high-level language complying with IEC 1131-3 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.

Statement List (STL): Statement List is a textual programming language resembling machine code and complying with IEC 1131-3.

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.