## Automation Requirements

| **Code** | **Application Field** | **Description** | **GMP relevant** |
| --- | --- | --- | --- |
|  | **Automation concept overview** | The machine control system must be composed of an operator panel, PC panel type, SCADA control system, and a PLC; all system servers shall be running on a virtualized environment.  The operator panel must communicate with the PLC and display information about it in the appropriate format in the prepared graphic pages.  The package control system must be linked to one automation control network to/for:   * + ICS DC: global ICS domain policies (Microsoft and ISA-99 recommendations)   + ICS NTP: time synchronization of all devices with time indication or time stamp   + ICS AD: global user management of all devices with "logins" (user accounts, passwords, and access control via AD global security groups)   + ICS FileServer: global data management of all devices generating data (centralised backups, archives, and user generated data)   + MES and Merck Data Historian: it must be possible to connect these systems | Yes |
|  | The SCADA design must be based on client / server architecture using Microsoft Remote Desktop Server technology (Terminal Host with applications). The SCADA clients must connect to the Terminal Host using RDP.  The SCADA shall be developed using Intellution iFix 5.8 by GE  Historian shall be developed using Intellution iFix 5.5 by GE. | No |
|  | The ICS design must comply with ISA-88, ISA-95, and finally ISA-99. | No |
|  | The package must be equipped with an HMI operator panels for the interface with the plant | No |
|  | Package vendor shall provide all instrumentation and control architecture starting from the fiber optic socket installed in the control package board.  Merck provides ICS backbone architecture and dedicated VMs with OS for the package units. Package Vendor shall supply, install and configure all application and auxiliary SW necessary in the VM environment at customer site. | No |
|  | **Operational**  **concept**  **overview** | All the HMI of the equipment will be client of the same SCADA application. Limitation of functionality on each machine to be implemented for safety reason will be set according the machine name. | Yes |
|  | For the purpose of harmonization between the existing Units and new Unit the Vendor shall submit symbol library of SCADA for approval. | No |
|  | **Operational**  **concept**  **overview** | The operator must see at any time the status of the equipment and for example which are the conditions the system is waiting for. | No |
|  | All equipment actuators shall be switchable in manual mode, selectable via the operator screen. | No |
|  | The equipment must be as much as possible “logical complete” to allow pass/fail results automatically. The result must be reported in the machine report and available for external system (MES and the future Historian system). | Yes |
|  | Power outage  The system shall be designed in a way to ensure that the system is able to maintain equipment monitoring during power failure in order to reduce impact on product. | Yes |
|  | Control system power  All systems components of control system must be connected to UPS power to ensure the reading of sensors and the interfaces.  In case of having actuators as well emergency powered the relevant output cards shall be supplied with UPS power as well. | Yes |
|  | **Virtualization** | The virtual environment will be provided by Merck; the virtual infrastructure is based on vSphare V.5.1 (or higher) and NetApp technologies. The Vendors will not have access nor configuration rights on vSpahre nor NetApp; the system configurations cannot be modified, these follow Merck IT Coorporated policies. | Yes |
|  | All servers must be virtualized. The Vendors shall foresee following components:  • Historian  • SCADA  • Terminal Server (based on Microsoft RDS)  The number of licenses shall be:  • the number of Thin Client installed on Machine and 3 (three) more license for the control room and maintenance. | No |
|  | The Vendor shall design resources for each VMs and fill the "ICS Server Hardware Configuration" table for the definition of:  • vCPU  • vRAM  • Local Disck C  • Local Disck E:  Operative system must be minimum: Windows Server 2012 R2 X64 (64-bit). In case there is a higher Windows version available before FAT, after consolidation with Merck the new version shall be used (Merck to verify integrity with ICD DC).  Only Windows Servers are allowed in Virtual, not Windows Clients. | Yes |
|  | **Alarms** | Vendor has to provide a document with a complete alarm list including the description of condition that generate the alarm, operation (in terms of recipe) dependence, description of action that should be performed to react on the alarm, and potential consequence of the alarm condition. | Yes |
|  | **Alarms** | Alarms and interlocks must be independent which means that disabling or changing a threshold to an alarm will not result in disabling or changing an interlock condition. | Yes |
|  | The software structure must follow the principle that if a command is given it is either executed or a message is raised if it can’t be executed reporting the reason. | Yes |
|  | Technical alarms and events causing the need for a maintenance person shall be grouped in priorities and/or kind of activities and made available for integration via dry contacts. | Yes |
|  | For each analog measurement, through appropriate dedicated windows, will be possible set the alarm set-point, for the following thresholds:   * + Low low value   + Low value   + High value   + High high value | Yes |
|  | Alarms shall be organized in priority groups. | No |
|  | Alarms shall be recorded in an alarm data table | Yes |
|  | Alarms shall be acknowledgeable individually or by priority group. | No |
|  | Alarms treatment and memorization shall be realized in the PLC. HMI/SCADA only shall visualize record and allow acknowledgement | Yes |
|  | Acknowledge and reset alarms will be through appropriate button, relevant actions will be recorded in a log file. | Yes |
|  | The functionality of acknowledgment and reset have the following meanings:   * + Acknowledgment: the acknowledgment of the alarm, which is available in the alarm video page with the lists of the alarms, will result in the termination of the flashing of the visual signal   + Reset: only “retentive” alarms need to be reset to restart the operating functions active before the rise of the alarm. However, to restart the system, it will be needed a dedicated operator command. | Yes |
|  | **Recipe management** | The package unit supplier should have ALL his parameter sets for ALL products under his “control”.  Either at SCADA layer or selectable data blocks direct in the PLC. For those package units which must handle files for other systems (e.g. inspection devices) this file management is as well part of the package unit vendor. Parameter sets and file (if applicable) shall be combined as package unit “recipes”. These PU recipes shall exist for all products.  The PU-recipes (and linked parameter sets and files) shall be selectable either from the package unit screen or remotely via MES. | Yes |
|  | The recipe management must comply with CFR 21 Part 11 requirements and ISA-88 and data integrity policies. | Yes |
|  | The decision from which source the selection is made (local or MES) is made via a “software” switch. | Yes |
|  | PU-Recipes shall be kept in a dedicated recipe data table.  PU-Recipe data structure shall at least include the following fields:   * + PU-Recipe name   + PU Recipe number   + PU Product name   + PU-Recipe version   + PU-Recipe approval flag   + PU-Recipe date   + PU-Recipe data | Yes |
|  | System shall allow recipe creation, saving and retrieval at SCADA level.  The recipe manager interface must be in compliance with CFR21Part11. | Yes |
|  | **Audit trails** | The System should create accurate and complete copies of audit trail in a standard form (, PDF). | Yes |
|  | Vendor shall implement proper audit trail method for all user activities as i.e.:   * + Log in/log out   + Log in failures   + Recipe creation / modification and approval   + Any parameter changes (i.e. tuning parameters, alarm levels, etc)   + Alarm acknowledgement   + Modes selection (automatic/manual)   + Any other manual actions (switch on/off machine, etc) | Yes |
|  | Audit trail should record each change executed on electronic records with relative metadata. | Yes |
|  | Audit trail should record each change executed on electronic records with relative metadata. | Yes |
|  | **Audit trails** | Audit trail file shall at least include the following:   * + Date & Time   + User ID   + Batch ID   + Parameter identification (tag and description)   + Action (action description)   + Old / new value)   + User comment where requested   + Approver ID and user comment (in case approval required) | Yes |
|  | In addition to be recorded in the Audit trail, if an operation requires an evaluation within the Batch report it must be communicated to the MES system.  In addition to be recorded in the Audit trail, if an operation or an event represents a deviation, this deviation must be communicated to the MES system. | Yes |
|  | The system must provide Audit trails report functionality. | Yes |
|  | Audit trail should not overwrite record changes on previously stored information | Yes |
|  | It should be possible to produce a complete Audit Trail printout | Yes |
|  | Audit trail should be exportable in a not alterable format. | Yes |
|  | Audit trail should be exportable in a legible format. | Yes |
|  | **Electronic**  **signatures**  **& records** | Critical record data shall be subject to authority check. | Yes |
|  | Common operations will not require dedicated signature but will use the actual logged in user as author. | Yes |
|  | Recipe approval and batch release will require electronic signature. | Yes |
|  | **Disaster**  **recovery**  **& back up procedure** | The Vendor shall provide a detailed document for disaster recovery measures/activities for all devices requiring configuration or setup after installation / replacement: Servers, HMIs, PLCs, any other local devices as drives, analyzers, etc. | Yes |
|  | **Disaster**  **recovery**  **& back up procedure** | The Vendor shall provide a detailed documentation for back up, archiving and restore strategy; design specification and user manual | Yes |
|  | Back up / Disaster recovery and Archiving / Restore for all control system shall not relay on ghosts or other manufacturer specific procedures, but should describe step by step all the set-up phases to rebuild an equipment from scratch. | No |
|  | The Vendor shall design the overall backup and archiving strategy according the following guidelines:   * + all devices that generates data must be identified by Vendor   + the devices must automatically generated backups once a day (time tbd by Merck)   + the backups must be automatically stored on a defined network location   + the backups (as per GxP) are meant for recovery of data after disaster (not to be confused with GxP archiving)   + large data bases are subject of archiving; archiving as per GxP cut the data from the active data base and exports for long term archiving   + the archives must be re-connectable / importable into the production system for data view (i.e. investigations) as per GxP requirements   + the archives must be automatically stored on a defined network location (different than the backup location). | Yes |
|  | The systems must be designed and configured to hold 3 years data online. Data older than 3 years shall be archived and moved to a predefined network location | No |
|  | **User Management** | The access of the users to the plants control system will be regulated through the Merck ICD Domain Controller.  Login must be connected to the ICS Domain Controller for user and password synchronization and global management of the security groups | Yes |
|  | The access levels of applications have to be the flexible. It must be based on functional security grouping, configurable in a centralized place (and not on every single button separately), i.e. in form of a matrix.  It shall be possible to assign different profiles for each user. | Yes |
|  | Merck User group for SCADA shall be as minimum:   * + Operator   + Supervisor   + Maintenance   + Administrator | Yes |
|  | All the equipment must be configured for time synchronization with Merck ICS Domain controller (this includes: servers, HMIs, OITs, PCs, PLC, scales and any other devices having system time). The systems must be setup for local time, including summer/winter time adjustment. | Yes |
|  | **Historian** | Full compliance with OSI-PI is required. | Yes |
|  | **Historian** | All process related data, alarms, and alert notification text is available for the OSI-PI Historian. | Yes |
|  | Full list of the PLC Tags for OPC Server Configuration must be provided | Yes |
|  | Meanwhile as the Merck Historian is not available yet, the equipment system must foresee its own historian systems that collects all process data, alarms and events, and audit trails. | Yes |
|  | The Vendor must ensure diagnostic and analysis of all components through secured remote access. The same applies to remote system maintenance and update.  The access to the Merck infrastructure will be granted following ISA-99 recommendations for secure access to control systems:   * + 1st level authentication (user logins to Merck Web page and establish a secure connection to Merck intranet)   + 2nd level authentication (user opens an RDP connection into ICS engineering server and provide credential of the control system). | Yes |
|  | List of all necessary software for a remote access for maintenance or upgrading system must be provided | Yes |
|  | **Cyber Security** | The Merck ICS DC blocks by default all "removable media" (i.e. USB ports) of Windows computers. This is a well-known Cyber Security measure in automation networks. In general, Vendor must block by design all "removable media" of any other non-Windows devices. | Yes |
|  | Windows Computers - Local Users and Groups:   * + it is not allowed to add any local users (domain users must be used instead)   + the default local Administrator password must be owned by ICS Administrator   + it is not allowed to add any kind of users or groups into local group Administrators   + it is not allowed to add Service Accounts into local group Remote Desktop Users   + it is not allowed to add personal user accounts to any local groups   + it is not allowed to add Domain Local Groups into any kind of local users or groups   + it is not allowed to start applications with auto-login users (app. must run as service)   + automatic logon Service Accounts must be assigned to local group Guests (not Users) | Yes |
|  | **Software** | All system will be in compliance with GAMP 5 | Yes |
|  | **Software** | Complete software development shall be based on the GAMP 5 guidelines | Yes |
|  | Before development of recording system, the data base structure shall be approved. | No |
|  | All graphical displays layouts shall be approved before test execution. | No |
|  | The SW supervision installed on board the various operator stations will be set up with a series of dynamic graphics pages, which enable operators to interface with the control system. The various pages will consist of at least:   * + Overview page with a selection of the part of the plant to display   + Displaying synoptic plant set up on the basis of the P&ID   + List of input and output signals   + Alarms management   + Management of the characteristic parameters trend   + Report management   + Log events   + Audit trail   + Control and sequence management   + Batch and recipe management | No |
|  | The synoptic plant graphics shall be animated based on P&ID. A simple scan of P&ID is not acceptable. The animation should consist of at least:   * + Visualization of actuator states with mode information   + Visualization of indicators and switches with mode information   + Visualization of device alarm states | No |
|  | Any interfaces shall provide a mechanism to monitor the communication (Life bit or equivalent). | No |
|  | All sequences will be described in the SDS | No |
|  | **Devices for emergency shut down or cut off** | The devices shall be installed where shut-down/cut-off is necessary in an easy accessible location. | No |
|  | The trip devices shall be red color and yellow background push buttons mushroom or palm type. | No |
|  | All devices shall be self-interlocked and contacts shall be normally closed type | No |
|  | The release of emergency shut-down/cut-off circuit cannot be done without manual reset of the trip devices. | No |
|  | **Devices for emergency shut down or cut off** | Hardware Interfaces (potential free contacts or galvanically insulated analog signals if required) shall be wired on dedicated terminals, one per equipment interface. (e.g. EMS, WFI, BMS terminals) if necessary | No |
|  | **Control Hardware** | Brand: SIEMENS   * + Model: S7-1500 | No |
|  | HMI hardware in all areas   * + Type: Touch screen 21.5" Full HD   + Brand: B&R   + Model: PC2100 | No |
|  | Control cabinet with 20% free space IP54 in AISI 304 | No |
|  | Media: Cat 6 STP for internal network and Optical Fiber (OM3 50/125, SC connector 1G bit/s) for the connection with Merck network cabinet | No |
|  | SWITCHES:   * + Siemens SCALANCE SWITCH XM400 shall be used for FO connection   + Siemens SCALANCE SWITCH XC200 shall be used for PLC/HMI/RIO connection | No |
|  | HMI network shall be TCP/IP Ethernet based. | No |
|  | HMI to PLC connection (if required) shall use Profinet. | No |
|  | **Instrumentation** | Preferred technology is in order of preference:   * + Profinet   + 24 VDC 4÷20 mA for transmitters 2 wire technology (0/4-10 voltage is not allowed).   + 24 VDC for switches   All analog inputs must be monitored for broken wire.  Other technology will be subject to Purchaser approval. | No |
|  | The instruments will be numbered according to Purchaser internal numbering system | Yes |
|  | **Instruments calibration, certificates and testing** | Instruments must be supplied with a manufacturer calibration sheet | Yes |
|  | For all instrument (analog, switches, etc.) shall be execute the instrument calibration as for calibration procedure, to be executed at production site after instrument installation. | Yes |
|  | **Instruments calibration, certificates and testing** | The calibration of the instruments shall be made using sample instruments that are certified according to NIST (or equivalent) and with NIST certificate (or equivalent) still valid. | Yes |
|  | Instruments must we wired in order to allow calibration without disconnecting the instrument, therefore cables must provide enough free loop to allow calibration at floor or scaffolding height. | Yes |
|  | VIT of Control system FAT of Control system | No |
|  | SAT of Control system | Yes |