AIM Addendum to tender - automation system requirements

Version	Date	Author	Description
01	27-04-2017	ANNI	First version
02	08-05-2017	KRNO	Formatting
03	04-07-2017	LULE	Chapter 5 modification: IT Security
04	03-10-2017	LULE	Update of chapter 4: Active part
05	26-01-2017	TOGA	Update of L1 part
06	05-02-2017	ADWI	Rework of document structure
07	26-02-2018	TOGA	Update of visualization system
08	27-02-2018	MASI	Proofreading
09	09-03-2018	ADWI	Update of Software Requirements
10	02-10-2018	TOGA	Update of PLC and Visualization part
11	17-04-2019	LULE	Changes in the part – active part, passive part (vendor)
12	08.08.2020	LULE	Cisco industrial swich IE series was added
13	30.03.2021	SZZY	Update of 4.1

Content

1. INTRODUCTION

The purpose of the Automation System Requirements document is to specify the overall system requirements that will govern the development and implementation of the system. The document describes initial system architecture, security considerations, project coordination methodology preferred by AMP. The main goal for the directives in this document is to enforce standardization of systems and infrastructure within AM Poland.
Standard hardware, platforms and procedures described in this document are baseline for all consultations if deviation from standards would be required by Contractor. Contact persons within Automation, Industrial IT and Models department (AIM) will be defined during the project and will be responsible for coordination and approval of project milestones within each responsibility.

2. ABBREVIATIONS

In this document below abbreviations will be used:

AM	ArcelorMittal
AMP	ArcelorMittal Poland S.A.
AIM	Automation, Industrial IT and Models (in AMP)
L1	Level 1 represents sensors, PLCs, SCADA systems
L2	Level 2 represents resources responsible for business logic
L3	Level 3 represents resources responsible for business logic, reporting
CONTRACTOR'S SOFTWARE	Shall mean any software, program and/or data-base, owned by the CONTRACTOR at the signature date of the concerned CONTRACT and necessary or used for operating, monitoring, maintaining the WORKS AND/OR EQUIPMENT or any part of them, as well as all operations relating thereto
SPECIFIC SOFTWARE	Shall mean any software, program and/or data-base developed and/or modified for the performance of any CONTRACT
STANDARD SOFTWARE	Shall mean any platform, operating system and/or data-base owned by a third party at the signature date of the CONTRACT and necessary or used for operating, monitoring, maintaining the WORKS AND/OR EQUIPMENT or any part of them, as well as all operations relating thereto

3. SOFTWARE

Each CONTRACT will specify the STANDARD SOFTWARE, SPECIFIC SOFTWARE and CONTRACTOR'S SOFTWARE to be provided or delivered under CONTRACT by the CONTRACTOR to the AMP. In case a software and/or program is not specified in the concerned CONTRACT as being either a STANDARD SOFTWARE or a CONTRACTOR'S SOFTWARE, such software and/or program shall be considered and construed as being a SPECIFIC SOFTWARE.

3.1. Standard Software

The CONTRACTOR shall deliver to AMP any and all STANDARD SOFTWARE as necessary for the performance of the concerned CONTRACT. AMP's rights to use the STANDARD SOFTWARE shall be assignable together with the relevant WORKS AND/OR EQUIPMENT. In addition, the CONTRACTOR shall, upon AMP's request and at no additional cost, provide the AMP with all information and **source code necessary to achieve the interoperability of other program(s) with the STANDARD SOFTWARE**. Expectations to this requirement should be discussed during negotiations.

3.2. Specific Software

The SPECIFIC SOFTWARE, including the related source code, shall belong to the AMP. Title to and ownership of the SPECIFIC SOFTWARE, including the related source code, and any related INTELLECTUAL PROPERTY RIGHTS, including author's rights and copyrights, shall be vested into the AMP. Expectations to this requirement should be discussed during negotiations. The transfer of ownership to the AMP of the SPECIFIC SOFTWARE, including the related source code, and any related INTELLECTUAL PROPERTY RIGHTS, including author's rights and copyrights, shall:

- occur at a price which is an integral part of the contractual price paid by the AMP to the CONTRACTOR as defined in the concerned CONTRACT;
- be applicable and valid in the country where the SITE is located as well as in all countries throughout the world; and
- be granted at least for the duration during which the concerned SPECIFIC SOFTWARE are protected by any INTELLECTUAL PROPERTY RIGHTS.

An exhaustive and updated copy of the source code of each SPECIFIC SOFTWARE shall be communicated to the AMP at any time, without any restriction of any kind, upon AMP'S first demand.

3.3. Contractor's Software

If the WORKS AND/OR EQUIPMENT include CONTRACTOR'S SOFTWARE protected in whole or in part by INTELLECTUAL PROPERTY RIGHTS, the CONTRACTOR shall grant to the AMP the entirety of the rights related to:

- operation, use, reproduction whatever the use and the process, on all existing or future supports(*);
- representation by all means and supports, including the transmission or via networks Internet/Intranet, edition, diffusion; (*) and
- adaptation, modification, correction, development, integration, transcription, translation, bearing (*),

(*) provided that the above-mentioned rights are necessary for the operation, maintenance, modification and/or use of the WORKS AND/OR EQUIPMENT. Expectations to this requirement should be discussed during negotiations.

The licence granted by the CONTRACTOR to the AMP as to the CONTRACTOR'S SOFTWARE shall:

- occur at a price which is an integral part of the contractual price paid by the AMP to the CONTRACTOR as defined in the concerned CONTRACT;
- be applicable and valid in the relevant country where the SITE is located as well as in any other country(ies) in which the WORKS AND/OR EQUIPMENT may be further moved, sold and/or transferred;

- be granted at least for the duration during which the concerned CONTRACTOR'S SOFTWARE are protected by any INTELLECTUAL PROPERTY RIGHTS; and
- include the right for the AMP to grant licences and sublicenses of such rights for the operation, maintenance, modification and/or use of the WORKS AND/OR EQUIPMENT.

The CONTRACTOR shall communicate to the AMP the method and know-how used to develop the CONTRACTOR'S SOFTWARE and those required to use the CONTRACTOR'S SOFTWARE with its best performance.
During the whole term of the CONTRACT and at least each three (3) calendar months (unless expressly otherwise specified the concerned CONTRACT), the CONTRACTOR shall deliver to the AMP and any future owners and/or users of the WORKS AND/OR EQUIPMENT an exhaustive and updated copy of the source codes of the CONTRACTOR'S SOFTWARE and all related documentation, the exhaustive and updated copy of the CONTRACTOR'S SOFTWARE's source codes having to be finally delivered at the PROVISIONAL ACCEPTANCE at the latest.

4. IT INFRASTRUCTURE

4.1. Servers and workstations

Contractor should preferably use server and client equipment or environment provided by AMP. Hardware requirements should be delivered by Contractor to AMP during the initial phase of project.

If proposed AMP server infrastructure does not meet Contractor requirements it is obliged to offer hardware equipment, servers, workstations and configurations which comply with AMP equipment and cyber security standards. The abovementioned hardware should be compatible with virtual environment in AMP AIM. Detailed configuration concerning e.g. processor, memory, drives, FC adapters, etc. is to be agreed on. All servers and clients should have the agents and services installed enabling integration of these devices in AD and allowing tools such as SSCM and SNOW to be deployed for all the systems delivered.

Each server and work station in AMP AIM should be consulted with and approved by AIM specialists.

Currently, the standard includes servers, disk arrays, FC switches and work stations: (Models are given by example, to be confirmed during the project) . Hardware has to come from polish distribution.

- Server used as virtualization platform:
  HPE ProLiant DL380 Gen10 8SFF or newer
  2 x CPU Intel Xeon-Gold min 3GHz
  512 GB RAM
  2x HPE SN1100Q 16Gb Single Port Fibre Channel Host Bus Adapter
  2x HPE Ethernet 10Gb 2-port SFP+ BCM57414 Adapter
  4xSFP+ 10Gb LR Transceiver
  2 x HPE NS204i-p Lanes NVMe PCIe3 x8 OS Boot Device
  HPE 2U Cable Management Arm for Easy Install Rail Kit
  HPE 2U Small Form Factor Easy Install Rail Kit
  HPE 5Y Foundation Care NBD SVC
  HPE DL38x Gen10 Support
  HPE iLO Advanced Electronic License with 3yr Support on iLO Licensed Feature
  2 x HotPlug Power Supply
- Virtual platform: **vmWare vSphere**
- Virtual Server **: MS Windows Server** – supply by AMP
- Array model: HPE, e.g. **HPE Primera A630**
- FC switch model: HPE, e.g. **SN6000B**
- **Workstation** (MS Windows 10 or higher) with **24'** monitor.

- High: intel core i7/16GB RAM / Storage 1: 128-256GB SSD, Storage 2: 1TB/External Graphics Card
- Standard: Intel core i5 processor/16GB/storage 500GB-1TB

- **Laptop** (MS Windows 10 or higher)
  - High: (Intel Core i7 / 16GB RAM/Storage 1: 256GB SSD, Storage 2: 1TB/External Graphics Card)
  - Standard: (Intel Core i5/16GB RAM/Storage 1: 500GB)
- **Thin clients**

All Printers are out of scope of this tender. Printers will be provided by ArcelorMittal Poland.
Any deviations from the standard must be approved by AIM.

4.2. Network

Contractor should use network infrastructure provided by AMP, when possible. Each new network in ArcelorMittal Poland should be designed (or consulted) and approved by AIM network specialists. Network topology will be provided by AIM, concrete cable paths can be designed by the contractor but **approval of AIM department is a must** (in order to ensure redundant paths via different cable tunnels etc.). Technical documentation and as-built documentation should be prepared along with physical and logic diagram, fiber split, fiber attenuation and comparison of reflectometry measurement of fiber optic lines. Logical address ranges for all devices will be provided by AIM department. Configuration will be done by AIM specialists (or should be done based on their directives). Segmentation via VLANS is obligatory, traffic filtering based on the firewall. Only **managed type network devices are allowed (switches, routers).** Repeaters and media converters are not allowed. The allowed brands of these components will be defined by AMP to comply with AMP standards. Types and concrete models proposed by the Contractor should be agreed with AIM specialists. Any works in cabinets are performed by the contractor (installation of devices, splitting of the cables, …).

4.2.1. Passive part

4.2.1.1. Fiber optical cabling

If there are no cable routes they should be designed in consultation with AMP personnel according to following rules:

- At both ends of fiber optic routes a spare cable should be left in accordance with the standard (5% of route per end - no less than 20 running meters). Spare cable mentioned should be put in a separate box or drawer (cabinet) or rolled up under elevated floor (if such exists). It is permitted to put spare cables from several routes in one box/drawer. Unless otherwise agreed the standard of fibers end should be SC – PC.

- Unless otherwise agreed a single-mode optical fiber from local manufacturer should be used. Minimum number of optical fibers cannot be lower than 24 in at least 2 tubes.

- Ends: all fibres should be welded (upon prior agreement, but only in exceptional cases it is allowed to weld a single tube).

4.2.1.2. Copper cables

If there are no cable routes they should be designed in consultation with AMP personnel according to following rules:

- Standard for copper cables (UTP/STP cable), sockets, patch panels: Category 5e or higher
- Copper cables should be split, at one end, in the cabinet on the RJ45 panel and on the user side in network socket 2xRJ45 (always two cables per socket)
- Spare cable at the network cabinet should be at least 2 running meters (cable excess is measured after installation of patch panel in the cabinet).
- Network sockets RJ45 (2 xRJ45 should be selected), preferred vendors: Molex, Modtap or Panduit
- RJ45 patch panels equipped with a tray and allow labeling, preferred vendors: Molex, Modtap or Panduit
- Cable organizers and fiber optic distribution boxes, preferred Vendor ZPAS
- Network cabinets (19”), cabinets should be equipped with power strips and ventilation panels, preferred vendor ZPAS
- Cable trays and ducts, wherever possible associated accessories (blank inserts, corners, …) should be used
- Minimum depth of cabinets is 800mm (other depths possible upon prior agreement)

All details must be agreed and approved by AIM.

4.2.2. Active part

Contractor should use network infrastructure provided by AMP, when possible. Design of active network must be approved by GMS in a course of technical discussions. Only manageable devices are permitted. The devices must come from legal sources. AMP S.A. must be the final registered user. Supplier is permitted to configure the devices only based on configuration templates provided by AIM.

Standard devices are as follows:

- Industrial network: CISCO IE series, Moxa, CTC, or Siemens
  (SIEMENS only upon agreement with AIM).
- Enterprise network: CISCO catalyst series or JUNIPER EX series.
- Wireless network: CISCO, HP ARUBA (other networks only upon agreement with GMN department)

Any deviations from the standard must be approved by AIM.

Detailed requirements for access devices, enterprise switch:

Access Switch	**General requirements for the devices, which should:** • be covered by at least 36 months (optimum support period for the devices is 60 months) or manufacturer's or partner's support. Update of software, replacement of damaged components and support in trouble-shooting should be possible during the validity of service agreement, • the manufacturer cannot have had declared end-of-support for configuration of the device offered by the supplier within the entire support period, • enable management using command line, access to the command line must be through a built-in local console port, and remote access using SSHv2 protocol, • support SNMP v2 and v3 protocol, • enable authentication using RADIUS, TACACS and local user base, • support marking and matching of packets according to 802.1p or DSCP, • enable queuing mechanisms with at least 8 queues per physical port, • enable installation in 19" cabinet, • enable use of optical modules supplied by a third party regardless of maintenance service purchased, • support automatic backup of configuration after each change of configuration or on demand, • support remote syslog server, • optionally support monitoring of operating environment (temperature, supply voltage, etc.).

	Technical requirements of access devices:
	• access ports using 10/100/1000 RJ45,
	• density of access ports should be from 8 to 12, 24 and 48 (to be agreed on),
	• at least 2 ports 1G SFP, SFP+ or XFP,
	• support of SPAN and RSPAN protocol or similar (same principal of operation),
	• all ports must be active i.e. must be ready to use without additional licenses,
	• all the above mentioned ports must work at full speed without over-subscription,
	• support for POE is optional (upon agreement)
	  ○ must be compatible with PoE+ and supply at least 350W power for connected devices
	  ○ in case of version with the lowest density of ports it must be compatible with POE+ and supply power to at least half of the access ports
	• support of 802.1X MAB protocol,
	• support of filtering by MAC address,
	• support of G.8032 protocol,
	• support of the following spanning-tree protocols: RSTP, MSTP, VSTP or equivalent,
	• support of 802.3ad (LACP) protocol,
	• should enable correct transfer of PROFINET frames,
	• support of 802.1q, security mechanisms (DAI, IP Source guard, DHCP Snooping, DHCP option 82, etc.).

Preliminary list of detailed requirements for wireless network:

Preliminary requirement for wireless network - consultation is mandatory	Any solutions which are based on wireless network will **be accepted only after proof of concept.** Wireless network must: • include design of AP layout and be consulted in scope of infrastructure, • include measurements of wave propagation and potential optimization of area coverage, • support security profiles assigned to SSID, • AP should have two independent radio channels working in MIMO technology, • AP should support all basic IEEE standards for wireless networks: 802.11 a/b/g/n (ac optional), • enable installation of external antennas (antenna socket), • set should include standard antennas, • enable automatic searching and adding AP to the controller, • enable construction of virtual wireless networks, • support 802.1q and 802.1p, • APs which are installed outside should be protected from weather conditions (hermetic cabinet IP65) or intended for an outside use, • support SNMPv2 and v3 protocol, • have a power supply compatible with POE or POE+ after prior agreements, • controller should support central authorization and authentication based on RADIUS (RFC2865), • generate information about network traffic in accordance with RADIUS Accounting standard (RFC2866), • support WMM standard in accordance with IEEE 802.11e, • offer a possibility to limit the throughput for a defined user group, • have the protections of wireless network: WEP, WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise and open network, • offer a possibility to support up to 500 active APs by one controller, • offer a possibility to support high-availability solution for controllers, • offer a possibility to install central controller in the network with central traffic flow system and local for selected installations (local traffic flow for selected SSID).

4.2.3. Fieldbus: Profinet/Profibus

- Preferred type of network as field bus is Profinet for connection between PLCs and IO islands, or between PLCs and industrial automation devices. Preferred network topology is ring (optical fiber cables), star in case of connections between Pofinet/Profibus devices series connections are allowable.
- Configuration of active network devices from PLC (HW config together with network topology).
- Rules for naming the individual slaves, cards and addressing should be discussed during initial design phase with AIM employees.
- Contractor is obliged to carry out quality tests of Profibus/Profinet network. Tests must be confirmed by a report for each subnetwork/node/ segment which should include:
    - List of devices to carry out measurements.
    - Communication statistics: attempts to establish communication, loss of communication, repetition of transmission, attenuation, signal level at the ends of segment, etc.
    - Detection of network topology.
    - Analysis of measurements.

List of detailed requirements for industrial switches:

Industrial Switch	**General requirements for the devices, which should:** • be covered by at least 36 months (optimum support period for the devices is 60 months) or manufacturer's or partner's support, Update of software, replacement of damaged components and support in trouble-shooting should be possible during the validity of service agreement, • the manufacturer cannot have had declared end-of-support for configuration of the device offered by the supplier within the entire support period, • enable management using command line, access to the command line must be through a built-in local console port, and remote access using SSHv2 protocol, • support SNMP v2 and v3 protocol, • enable authentication using RADIUS, TACACS and local user base, • support marking and matching of packets according to 802.1p or DSCP, • enable queuing mechanisms with at least 8 queues per physical port, • enable installation on DIN bus or in 19" cabinet, • enable operation in the extended range of temperatures 0°C…+50°C (option:-40°C…+70°C), • enable use of optical modules supplied by a third party regardless of maintenance service purchased, • support automatic backup of configuration after each change of configuration or on demand, • support remote syslog server, • optionally support monitoring of operating environment (temperature, supply voltage, etc.), • device should be able to operate in an environment with high level of dust (no fans, protections of unused ports, etc.).

	Detailed technical requirements for industrial access devices: • access ports using 10/100 Mbps RJ45 (option: 10/100/1000 RJ45), • minimum 6 to 8 access ports (exact number as per agreements), • at least two 1G SFP ports, • support of SPAN and RSPAN (option) protocol or similar (same principal of operation), • all ports must be active i.e. must be ready to use without additional licenses, • all the above mentioned ports must work at full speed without over-subscription, • compatibility with PoE+ (option, as per agreements), • support of 802.1X MAB protocol as an option, • support of filtering by MAC address, • support of G.8032 protocol (other ring protocols are permitted but ITU standard is preferred), • support of the following spanning-tree protocols: RSTP, MSTP or equivalent, • support of 802.3ad (LACP) protocol, • should enable correct transfer of PROFINET frames, • should enable quick configuration in case of breakdown (restoring configuration, auto configuration, etc.), • should enable DC 24V or 48V power supply (to be agreed, optionally, from two independent feeders), • support of 802.1q, security mechanisms (DAI, IP Source guard, DHCP Snooping, DHCP option 82, etc.), • increased resistance to overvoltage on camera power supply line, • should enable QoS marking on access port.

5. LEVEL 1: BASIC AUTOMATION ENVIRONMENT

Control system should enable in a reliable way:

- Process control
- Processing of measurement data
- Visualization of statuses and processes
- Data archiving
- Recording of any selected input signals or secondary signals generated in the system
- Diagnostics: alarms, warnings, operator events, breakdowns of industrial network, malfunction of servers and operator stations

5.1. PLCs

Preferred standard for PLCs in AMP are Siemens S400 or 1500 PLCs (process line PLCs) and S7 300 or 1200 (in case of package installations). Selection of PLC series is done after agreement with AIM. For scattered stations Siemens ET 200MP or ET 200SP is a standard solution. It is recommended to use modules offering Shared Device functionality. Use of any other scattered

stations only upon agreement with AIM. Supplier should ensure unification i.e. use one type of CPU, CP, PS for each series. Version of utility software, Simatic Manager or TIA Portal, should be agreed with AMP. Allowable size of work memory utilization in PLC is 60%. Maximum time of OB1 cycle is 150ms.

All PLCs should be in one multi-project, if possible, together with HMI projects. In case of Simatic Manager (PLC) or TIA Portal (HMI) software, Device Proxy functionality should be used.

Programs in PLCs should be written according to strictly defined rules and criteria, and use common library. Requirements and rules should be agreed on during initial design phase with AIM employees.

All PLCs should be available from engineer station, including configurable network devices, measuring and operating elements if it is possible to connect them to network and manage them using PC/WWW application.

Contractor will supply source codes and documentation of all libraries used. It means that there should be no element of the system for which the source codes are not provided, excluding standard Siemens library blocks. Source codes should be written in a clear way with comments in English and/or in Polish. Expectations to this requirement should be discussed during negotiations.

PLCs should have automatic backup of modified parameters (e.g. process settings, regulators, alarm thresholds, etc.) so that CPU starts-up with current parameters after restart or reset.

System should enable its easy expansion by adding new modules or stations, devices.

When the system is handed over for use each of its components (CPU, CP, active network devices, etc.) should have the latest stable firmware (same for each type) installed.

S7 PLCs and manageable network devices should have time synchronized with HMI servers, L2 or time server indicated by AMP. Events generated by PLC program should be organized in a hierarchical manner (avoiding generation of unnecessary alarms resulting from other alarm e.g. power supply shutdown should not generate additional alarms e.g. about losing the confirmation form valves when they are supplied from this circuit.)

PDC (Process Data acquisition Centre) developed by ArcelorMittal is considered as main tool in AMP to be used for process registration, analysis and processing of measurement data, from PLC and/or other devices. All new installations should be so designed to be “PDC ready”. PDC is communicating with L1 devices using TCP/IP network and proper drivers device dependent.

Some of the PLC/devices require implementation of special logic and/or hardware configuration to allow data exchange with PDC (for example for S7-400 – additional connection definitions are required, functions, data blocks, etc..). PDC could have impact on PLC cycle, memory usage and network capacity, which are PLC/devices and project dependent factors, all of them need to be considered in project planning. For details consultations with AIM department are necessary.

5.2. Safety program

Risk analysis should be made at the project preparation stage and introduce safe solutions in the base automation systems.

Integration of standard program and safety program within one PLC (one system, one data bus, one engineering for standard and safety automation) is a preferred solution.

Safety program should be based on a family of safety PLCs, Simatic Safety Integrated. F-LAD, F-FBD and integrated and certified (TÜV) function blocks should be used to write a program.

Safety inputs and outputs will be connected to distributed ET200 stations by means of appropriate fail-safe modules.

Rules for the scope of library blocks, naming of the individual cards, configuration of DIP switches and addressing should be discussed during initial design phase with AIM employees.

Each of the components of safety system should have a standard diagnostics: emergency stop, ambiguity between channel 1 and 2, required test after passivation, required confirmation, passivation, etc.

Safety program should be based on safety matrix which includes all safety system components (E-stop buttons, S-Stop, barriers, doors, sensors, etc.), clearly defines the cause and effect for control system.

Matrix must be visualized in SCADA system.

Prior handing over the system for use the Contractor is obliged to run the tests of safety program. Tests should be performed in accordance with current safety matrix. Tests should be performed in the presence of AMP employees and their completion must be confirmed by an appropriate report including date, time, control sum of safety program, components tested and their effect on control system.

It is forbidden to use markers to by-pass safety signals; safety output signals must include safety input signals.

Safety data exchange between PLCs can be done only over safe channels e.g. Profisafe.

5.3. Visualization

Standard to be used for SCADA systems is Wonderware System Platform 2017. In justified cases it is allowed to use InTouch 2014R2/2017 SCADA (e.g. upgrade of older InTouch versions) but only upon agreement with AIM. Deviations from the standard are acceptable only in special cases (local unification of solutions) after receiving positive opinion from AIM. System should have client-server architecture with redundant servers.

Control should be available from operator stations. Client applications should be launched from Operator's account. Launching from Administrator's account should not be possible.

Applications should start automatically without any manual actions of the personnel i.e. when the power supply is on the system log-ins automatically to the Operator's account and launches client application.

Configuration of operator stations should be the same. Each station should enable control and monitoring of the entire production process.
Defined appropriate user groups having the rights to control and change process parameters.
Observation of measurement trends from the system must be available on all operator stations
Possibility to view historical data. For each variable it should be possible to enter time horizon of archiving (e.g. from the last hour, day, week).
Archiving of measurements data should be agreed with AIM.
Colors of SCADA elements and layout should be in line with standard effective in AMP.
Entire SCADA design should include same elements i.e. same font for all the descriptions; colors and sizes of repeatable elements should be the same as well.
System must be in Polish language (description on graphic images, alarm messages, etc.)
Data update time on the operator screens and time of changing the operator masks should not be longer than 1s.
System elements which are similar i.e. pumps, valves should have variables grouped using structures.
All repeatable elements i.e. pumps, valves, analogue measurements, regulator control pop-ups should be done using templates of control pop-up/faceplate.
Detailed visualization after opening control pop-up/faceplate. Current status, possibly to control in a manual mode, alarms, warnings also historical and e.g. current posirion, current and set-up speed, operation time, number of starts, current, voltage, detailed diagnostics e.g. error codes with support system, possibility to open current electrical documentation (in pdf format) regarding the device presented on the control pop-up.
Detailed visualization of interlocks of individual devices, group of system devices with a possibility to make a by-pass by operator having proper rights.
Visualization of sequence, switching conditions and their logic as well as operations performed in specific steps with possible manual intervention of operator (proper rights makes it possible to force switching to the next step, stopping the sequence, etc.).
Names of variables in SCADA system must correspond with names of variables in PLCs as well as electrical and process documentation.
Visualization of safety system:

- each element of safety system: E-Stop button, S-Stop, curtain, barrier, doors, sensor, etc. must be shown in a general view of system in an installation location with accurate description of location (cabinet, pulpit, etc.)
- safety matrix visualization showing causes and effects for each element of safety system.

Event system should meet the following requirements:

- One consistent system for handling events covering strictly defined event classes (e.g. alarms, warning, technological malfunction, system malfunction, operator event, etc.).

- System events handling (e.g. station statuses, correctness of module operation, communication errors, etc.)
- Recording of operator events: each action activated by a button, switch (e.g. change of operating mode, start/stop and turn on/off command, selection, etc.) on HMI operator station, local panels and local control boxes should be recorded as an event.
- Presentation of events in a form of freely defined lists (e.g. process area, type of device, event class, etc.).
- Presentation of events should be clear in Polish language, length of messages should enable clear description of event (avoid abbreviations)

Visualization and diagnostics of industrial networks (Profinet/Profibus of specific PLCs, PlantBus, TerminalBus) showing current topology of network with network status.

Visualization of energy system: power supply monitoring, switches, fuses, UPSs, etc.

Contractor must foresee licenses for utility and application software, as well as include at least 30% of spare over the variables used while performing the project.

6. LEVEL 2/3 SYSTEMS

Table and information in this topic provide design constrains requirements for Level 2 systems developed during the project:

- C# will be basic programming language and only in justified cases, programs can be created using C++
- .Net framework 4.5 (or higher) should be used
- The mandatory database is MS Microsoft SQL Server, any deviations from this standard should be agreed upon with AIM
- Standard client operating system (MS Windows 10 Pro 64)
- Standard server operating system (MS Windows Server Platform)
- Client – Server model architecture should be implemented.
- System should be fault tolerant and scalable
- User access management tools must support roles, groups methodology, with possibility to integrate with MS Active Directory Domain.

Contractor will provide all source codes and development and installation scripts for all software, which cannot be purchased from other supplier unrelated to the Contractor. This means that there **can be no black boxes** in the system, except for operating systems. Expectations to this requirement should be discussed during negotiations. Tools should ensure fast error diagnostics during acceptance and during operation.

Level	Layer	Function	Standard	Tools	Langu-ages
L3/L2	**Business layer applications**	Use of basic objects (for core objects)	Windows Services, WCF	.Net, Visual Studio	C#, C++
		Tasks (Jobs)	SQL Server 2014	.Net, Visual Studio	SQL
		For file configuration	XML	.Net, Visual Studio	XML
	Database solutions	Database solution	SQL Server 2014	SQL server management tools	SQL
		Designing of reports	Microsoft Reporting Services	SQL server management tools	SQL
		Communication with databases	ADO	.Net, Visual Studio	C#, C++
	Client layer applications	Operator interface	WPF	.Net, Visual Studio	C#
		User data files	XML	.Net, Visual Studio	XML
	WEB Presentation	WEB communication	WCF	.Net, Visual Studio	C#
		Users interfaces	ASP.Net	.Net, Visual Studio	C#
	Communication with L1	Communication with L1 (PLC),	TCP/IP Socket	Visual Studio	C#, C++
	Communication between applications	Exchange of information between components	WCF (preferred), TCP/IP Socket,	.Net, Visual Studio	C#, C++
	Communication with external systems	Communication other systems	WCF (preferred), TCP IP Socket	.Net, Visual Studio	C#, C++

7. IT SECURITY

Company and the contractors implementing IT infrastructure and OT-related projects must be aware of the cybersecurity issues. Remote access for external companies is only allowed in justified cases in accordance with AM Poland policies (connection via VPN concentrator and rebound server; necessary access and specific people who will be able to use remote connection will be approved by guarantor from AMP). No possibility to provide direct network connection to the devices. Contractor will not include in the network any devices which enable remote access. Devices with direct access using mobile networking technology (e.g. 3G or 4G) are also forbidden. This rule applies to all project phases (from engineering up to normal operation). Special attention is to be paid to the devices with "hidden" networking capabilities such as printers, air conditioning equipment, etc. (e.g. Internet of things). Any need for external access to the network will be discussed and solutions will be suggested by AMP AIM or IT Security Officers.

Devices supplied for the projects should be covered by manufacturer's support. Use of 2 network cards is prohibited. Each server, network device should be added to monitoring system via SNMP. IP addressing, rules for device access to other systems and subnetworks (including OT connections to internet and corporate network) are approved and defined by AIM specialists. Separation of services and management at network level is recommended.

Physical access: servers and network devices should be located only in the areas intended for this purpose where proper conditions are ensured (access control, air conditiong, fire extinguishing systems, etc.). Those areas should be indicated and agreed on with ArcelorMittal Poland employees. It is recommended that operator stations are locked in the cabinets. Virtualization environment has to be used (servers). Desirable technical approach: Virtual server/servers and thin clients instead of typical workstations.

All work stations and servers should be **added to PA.AMP domain** (or ISPATCEE, depending on purpose of the system). Applications on work stations should not run using administrator's account; default system accounts (guest, administrator) should be disabled. Passwords must meet AMP security standards and should be changed in accordance with current security policies. Accounts with administrator rights in Windows system (or other operating system, if applicable) can be used only to install software. Hardware and software configuration (firewall, computer name, users, etc.) should be done by AIM specialists (or at least agreed with them).

All users should have a separate account to log into the Windows system and software supplied by the Contractor. All exceptions (HMI, other systems directly related to the industrial processes) must be justified in detail and approved by AIM specialist. Applications supplied by CONTRACTOR mustn't use root accounts and should use PA domain authentication as well

All systems should have antivirus software defined by AIM. Currently used program is McAfee. McAfee Virus Scan Enterprise (or EndPointSecurity) as well as McAfee agent should be installed on each system/work station. System should enable on-line update of antivirus database (ePO server) and normal

operation of the system and software should not be affected by the real-time antivirus scanning. Details must be specified together with AIM specialists. USB ports on work stations should be disabled. No internet connection in production environment.

Each application server supplied by the contractor (client applications only if necessary - to be agreed on) should be archived by Central Automatic Backup System, which is managed by AIM. Acronis agent must be installed on each archived system. It has to be evaluated whether the current system resources will allow for making back-ups. In case of shortage of resources they need to be added e.g. arrays, licenses, etc. Schedule of back-ups should be agreed on with the representative of a given AIM group and system recovery test should be performed. If it is not possible to do automatic back-ups using Acronis agents e.g. due to lack of proper network infrastructure the system should be archived manually. In this case it is necessary to plan actions aiming at starting the automatic system archiving and define planned start date. All systems should enable installation of agents of software like SNOW, SCCM.

Each system must enable updates of the STANDARD SOFTWARE (e.g. Windows operating system or database updates, etc.). Client/server applications should enable regular patching of systems - in case of problems with installing the updates the company/supplier of software agrees to modify it to enable regular patching of operating system. Systems should be updated via WSUS server/SCCM. Additional agents will be installed in the system: SNOW, SCCM and others if necessary (to be discussed with AIM specialists).

8. PROJECT COORDINATION

AIM should be involved in all phases of the project in such a way that they have full knowledge of the current status of the works in the automation area. This means that meetings in the Contractor's offices will be held on regular basis to gain a detailed insight into the status of the project and discuss the proposed solutions. Additionally, AMP engineers should be allowed to take active part in all steps of the development process, i.e. analysis, design, programming and testing. The preferred way to achieve sufficient involvement is the so-called “mit-arbeit”, where AMP specialists are integrated in the supplier’s teams as co-developers.

Each stage of project should have adequate planning and documentation. Before starting the project the following has to be agreed on:

- Documents distribution and updates methodology
- Files format

The following documentation should be provided by the Contractor (minimum requirement). Additional requirements will be discussed during initial phase and/or detailed engineering.

Initialization phase deliverables proposal:

- Complete architecture diagram and concept of control system

- General overview of the system: description of all system components, algorithms, parameters, network, etc.
- Functional description of all components: principle of system operation under normal operating conditions and in alternative operating modes
- Project Plan

Detailed engineering deliverables proposal:

- Complete system functional specification
- IT Infrastructure design document
- Level 1 design
- Level 2 design

Development deliverables proposal:

- Complete system development specification
- Level 1 development specification
- Level 2 development specification
- Test Plan

Test and acceptance:

- Test Results
- Operation manuals, including description of operating modes and possible measures to resolve the incidents.
- Operation manual for AMP process operators including the description of visualization system, processes and reporting function
- Maintenance and service manual including the principles of diagnosis. Operation manual should describe the systems installed, their operation, diagnosis and troubleshooting procedures, as well as system operation procedures. Documentation should allow AMP personnel to operate the system without any external support.
- Procedures for installation, backing up and restoring data, development of the system, etc.

Commissioning Phase:

- Documentation of application software, including utility, system and service software,
- Rules used in the project such as color conventions, programming guidelines, naming conventions, etc.
- Network and hardware infrastructure technical documentation and as-built documentation should be prepared along with physical and logic diagram, fiber split, fiber attenuation and comparison of reflectometry measurement of fiber optic lines.
- Operation and maintenance manual for hardware installed,

- Description of communication protocol implementation and the list of data telegrams, which are used inside the system and for external communication
- Documentation containing: version numbers of system and application software of PLCs and modules, serial numbers of system components, PLC configuration version numbers
- Contractor will hand over as-built documentation including all the changes made in detailed engineering. Documentation should include copies of declarations of conformity certified to be true by the Contractor for equipment installed, as well as reports from measurements

NOTE: Documentation must be prepared in a way that enables further development and modernization of the system independent from the Contractor.

8.1. Tests and Acceptance Guidelines

Testing environment should include a functionality covering the task being executed and should be available as a training environment for operators. This simulation environment should be able to simulate normal operating conditions as well as exceptional situations. Description of tests will be agreed upon between AMP and the Contractor during detailed engineering. As a principle, these tests should convince AMP that the project is mature enough to be implemented in AMP.

During FAT test the Contractor ensures that they will prepare infrastructure which enables preparation of network and hardware configuration in scope of PLCs, HMI computers, switches, etc. Preparation of required simulation of specific facilities and devices to reflect normal operating conditions and exceptional situations. Acceptance will be given by AMP personnel.

FAT tests should be carried out in the Contractor's plant/workshop prior delivery of automation system to the plant. The goal of the tests is to confirm readiness of the system to be installed and commissioned in the plant. Plan of FAT test will be provided by AMP. Contractor will provide the description of system operation before conducting FAT test. The description should include:

- functional description of individual system elements (device function, operating principle, operating mode, interlocks, etc.), automation description including description and diagrams of sequences.
- project documentation: project structure, description of library blocks used, communication interfaces betweem PLCs and package installations and L2.
- HMI documentation: configuration, navigation, alarm system, description of used control pop-ups/faceplates, historical data, etc.
- documentation of Profibus/Profinet network of individual PLCs and industrial network (PlantBus – PLC network, TerminalBus – HMI network).
- complete electrical documentation,
- complete source software defined at this stage of the project

Once the equipment is on site, all functional tests will be performed by the Contractor. Contractor will provide AMP with a confirmation that the tests were performed.

Test scenarios for software and hardware safety (e.g. emergency stops, shutdown and lockout mechanisms) will be defined by the Contractor. The scenario will include all safety components and the entire chain in the so-called validation tests. Tests will be carried out in the presence of AMP personnel and their completion must be certified. Any safety-related changes to the software or hardware require revalidation of a given part.

8.2. Training Scope

Expected training sessions:

- training for operators and maintenance personnel in tools/environment and the software,
- training for system administrators in tools/environment providing administration tasks,
- training for automation personnel, training should provide a sufficient level of detail so that AIM personnel can make all possible changes in the software (e.g. to add or expand interfaces, change logic, change/add user interface, etc.).