



Technical Standard

Date October 1, 2021

Ref. No MEIA0015

Page 1 (24)

Mondi AG.

Mondi Standard Harmonization

OPERATIONAL TECHNOLOGY (OT) INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) SPECIFICATION

Contents	1	General
	2	Systems scope
	3	Recommended manufacturers
	4	Power distribution and earthing
	5	Network cabling and cabling systems
	6	Networking principles
	7	Networking
	8	Industrial control network components
	9	Communication links
	10	Site environment
	11	Systems
	12	Software
	13	ICT infrastructure
	14	Trustworthiness
	15	Hardware requirements, scalability and compatibility
	16	Usability, administration and support
	17	Systems design and implementation

Distribution

Mondi, AFRY

Orig.	01.10.2021 / PKa, AFRY	01.10.2021 / EP, AFRY	01.10.2021 / LCa, AFRY	01.10.2021 / LCa, AFRY	Original issue
Rev.	Date/Author	Date/Checked	Date/Approved	Date/Issued	Notes

ABBREVIATIONS

A&E	Alarms & Events
AC	Alarm and Conditions
AC	Alternative Current
APL	Advanced Physical Layer
ARP	Address Resolution Protocol
BAS	Building Automation Systems
CWS	Corporate Workstation Standard
DA	Data Access
DC	Direct Current
DCS	Distributed Control System
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
e.g.	exempli gratia, for example
EN	European Standards
EU	European Union
FE	Functional / Telecom Earth
GDS	Global Discovery Server
HA	History Access
HART	Highway Addressable Remote Transducer
HAD	Historical Data Access
HMI	Human-Machine Interface
I/O	Input/Output
ICMP	Internet Control Message Protocol
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IEC	International Electro technical Commission
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISA	International Society of Automation

ISO	International Organization for Standardization
KMS	Key Management Service
KVM	(field connections to these systems shall be IP KVM)
LAN	Local Area Network
LEED	Leadership in Energy and Environmental Design
LTE	Long Term Evolution
NFC	Near-field communication
NIC	Network Interface Controller
NTP	Network Time Protocol
NTS	Network Time Server
ONVIF	Open Network Video Interface Forum
OPC UA	Open Platform Communications Unified Architecture
OSDP	Open Supervised Device Protocol
OT	Operational Technology
PE	Protective Earth
PN/PN	Profinet/Profinet
PoE	Power over Ethernet
PTP	Precision time protocol
RMON	Remote Monitoring
SAT	Site Acceptance Testing
Scada	Supervisory control and data acquisition
SIA	Security Industry Association
SIS	Safety Instrumented System
SNMP	Simple Network Management
SPE	Single Pair Ethernet
TCP	Transmission Control Protocol
TN-S	Terra Neutral Separate
TSN	Time-Sensitive Networking
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
VDC	Volts Direct Current
VLAN	Virtual Local Area Network
WiFi	Wireless Fidelity
XML	Extensible Markup Language

1 GENERAL

1.1 Purpose

This document defines the general principles for information technology in operational technology systems. Application of standardised technologies and procedures given in this document and specific instructions and descriptions are given in separate specifications for each system. Such systems are for example:

- Scada,
- DCS
- SIS
- machinery or actuator related controls (cyber physical system)
- embedded ICT
- production control
- site monitoring systems
- building management systems
- maintenance management
- data network

All these (and others similar) shall be called systems later in this document.

The document is intended for all Suppliers supplying systems with ICT as

- embedded solutions,
- application or
- services

separately or as part of equipment, sensors, actuators, IoT devices or other package.

Any deviation from these instructions in project proposal or delivery shall be notified by Supplier and will be allowed only with a written agreement by Mondi. The selection of applied technology where this instruction gives possibility for choice shall be given in the appropriate enquiries and separate project instructions.

1.2 Systems Specifications

All equipment shall be according to the standards and Purchaser's instructions. All ICT equipment, software and licences included in the system must be approved by Purchaser. The systems shall be upgradable with predictable life cycle cost.

The plants operate continuously throughout the year. It must be possible to repair a piece of equipment without interrupting the processes. Special attention must be paid to easy replacement of faulty devices and components. Redundant units securing the resiliency of the process and machine safety and general trustworthiness of operations shall be used where needed.

1.3 Codes, Regulations and Standards

The design and specification of the systems shall be in accordance with applicable local laws and regulations, and local codes and ordinances and specified codes and standards.

It is Supplier's responsibility to inform himself of the applicability of any mandatory codes and regulations and to certify to Purchaser that the supplied hardware and software conforms to those requirements.

The work shall comply with the standards, recommendations, stipulations and safety instructions currently in force in location and Purchaser's site standards.

Where applicable the equipment and installation shall comply with the following standards, regulations and instructions:

- IEEE recommendations
- International Organization for Standardization (ISO)
- International Electro technical Commission (IEC)
- European Standards (EN)
- International Society of Automation (ISA)
- Leadership in Energy and Environmental Design (LEED)
- Laws and regulations currently in force in site location
- Local authorities' regulations and recommendations
- Project instructions (will be partly delivered during the projects)
- RoHS 3 (EU 2015/863)
- Local disability / accessibility act

1.4 References

EN 50173	Information technology, Generic cabling systems
EN 50174	Information technology. Cabling system installation
EN 50346	Information technology. Cabling installation. Testing of installed cabling
IEC 60269	Low-voltage fuses
IEC 60364-5-54	Low-voltage electrical installations - Part 5-54: Selection and erection of electrical equipment - Earthing arrangements and protective conductors
IEC 61131-3	Programmable controllers - Part 3: Programming languages
IEC 61499	Function blocks
IEC 61850	Communication networks and systems for power utility automation
IEEE 1588	Standard for Precision Clock Synchronization Protocol for Networked Measurement and Control Systems
IEEE 802.1p	Strict Priority
IEEE 802.1Q	Standard for Local and Metropolitan Area Networks - Bridges and Bridged Networks

MEIA0002	Recommended Manufacturers for Electrical and Instrument Equipment
OT-SP_v1.1a	OT-Security Policy Category “A” Sites, Mondi Group IM
OT-TS_PROFINET_v1	Technical Standard PROFINET, Mondi Group IM

2 SYSTEMS SCOPE

The scope of systems is specified in the technical and commercial specifications of the contract or order. The technical specification includes equipment, software and licence lists of the systems with delivery limits and delivery limit diagrams.

3 RECOMMENDED MANUFACTURERS

Supplied equipment shall follow the separate standard Recommended Manufacturers for Electrical and Instrument Equipment (MEIA0002).

4 POWER DISTRIBUTION AND EARTHING

4.1 Power distribution

The power supply shall be 400/230 V 50 Hz, TN-S system.

Uninterrupted power shall be distributed from centralized, redundant UPS power supply units over a special UPS power network. The UPS units shall be connected to the (IP) data network and monitored.

4.1.1 Systems Internal Power Distribution

The internal power distribution of systems shall be coordinated with Purchaser's electrical designer to retain the selectivity of network protection. In general, the tripping current curve of miniature circuit breakers in systems shall be Type B. Possible internal fuses shall be according to IEC 60269 (Low-voltage fuses) gG and trip in less than 0,2s in UPS supply cases and in less than 0,4s in non-UPS supply cases.

Service power strips shall be equipped with residual current devices (A-type, 30 mA).

4.1.2 Power Distribution in System Rooms and Site Electrical Containers

As part of electrical power distribution, one supply of ordinary site power and one redundant supply from the Site UPS shall be provided in each location (electrical room / container, server room, rack room).

Larger systems with hardware units shall contain power distribution cabinets for internal power distribution. Necessary isolating equipment and battery units shall be integrated in the electronic cabinets to guarantee the required availability and quality of the supply power. All these systems shall contain necessary switches, fuses and/or breakers and terminals for the system's AC power distribution.

The systems shall contain required switches, fuses and/or breakers, power supply units and terminals for the system's internal DC power distribution (if not included in other cabinets).

4.1.3 Power Distribution in Control Rooms and Offices

Fixed power outlets shall be planned and installed in the control rooms and offices for the desktop electronic equipment (work stations, telephones, printers etc.) as part of the building electrification. The site systems' user equipment shall be connected to two separately fed UPS distribution outlets.

4.1.4 Power Distribution in Field Enclosures

AC power distribution shall be separately planned and installed to the field enclosures as required by the networks, buses, field equipment and auxiliaries.

4.1.5 Power over Ethernet (PoE)

Power over Ethernet shall be used to provide power to selected equipment (WiFi access points, cameras etc.) with data on Ethernet cabling. The power shall be fed with PoE enabled active devices. The supplier of the systems to be powered shall give the necessary PoE level required. The Purchaser data network designer shall specify the active devices, cabling and connectors.

4.2 Earthing

In general, instructions given in IEC 60364-5-54 (Low-voltage electrical installations - Part 5-54: Selection and erection of electrical equipment - Earthing arrangements and protective conductors) on application of equipotential bonding and earthing in buildings with information technology equipment, shall be followed in designing the earthing for ICT systems and equipment.

4.2.1 Earthing in system rooms

As part of site equipotential bonding and earthing one PE (Protective Earth) and one FE (Functional / Telecom Earth) earthing bus bar shall be provided in each system room (electrical room, server and computer room, rack room).

Electrical equipment in ICT systems shall be connected to the site protective (PE) and functional earthing (FE) network on the site. The systems supplier shall take care that the protective ground and signal ground are kept separate in his equipment.

4.2.2 Earthing in Field Enclosures

Earthing shall be planned and installed to the field enclosures as required by the networks, buses, field equipment and auxiliaries. The instructions given for applied technologies shall be followed.

5 NETWORK CABLING AND CABLING SYSTEMS

Directives and instructions given in EN or equivalent ISO/IEC standards relating to ICT cabling and cabling systems shall be followed:

- EN 50173, Information technology, Generic cabling systems.
- EN 50174, Information technology. Cabling system installation.
- EN 50346, Information technology. Cabling installation. Testing of installed cabling.

Cables shall be selected according to the cable standard MEIA0005.

6 NETWORKING PRINCIPLES

6.1 Connections to Site Network

Site network main structure with connections and subnetting, shall be given in a separate Purchaser issued technical standard for OT ICT Structure, Sub-netting and Addressing.

6.2 Network Connected Devices

Network settings of all network-connected systems and equipment shall be agreed upon with and approved by Purchaser.

All systems, workstations and servers shall be synchronised to Purchaser's time server with NTP (Network Time Protocol). The required NTP-clients shall be included in the systems. The network time server (NTS) will be part of the Purchaser site systems.

For time-critical systems requiring sub microsecond skew in geographically distributed systems the IEEE 1588 (Standard for Precision Clock Synchronization Protocol for Networked Measurement and Control Systems) precision time protocol (PTP) shall be used.

Normal Ethernet adapter cards shall be 10/100/1000Mbps (autosensing with a selection to be locked) and equipped with RJ45 twisted pair connectors. There must be an option to use 10 GB network cards.

Servers shall be equipped with Ethernet cards with dual ports for redundant connection to the network (teaming).

6.3 Wireless

All wireless networked systems (Wifi) shall use wireless networks implemented by Purchaser.

Special safety and security related wireless solutions shall be secured and implemented as given in the directives for the applied solution. See also Purchaser's OT-Security Policy Category "A" Sites (OT-SP_v1.1a).

Communications using radio frequencies shall be implemented as described in the separate Purchaser issued technical specification for wireless local area communications.

6.4 Protocols and communication

On the Network layer IP (and ARP) providing the mechanism to address and manage data packets being sent to nodes on the network, shall be used.

On the transport layer TCP, (and as necessary UDP, ICMP and IGMP) shall be used for controlling the application level services between network nodes.

IPv4 shall be used in all systems, IPv6 services shall be disabled in all network equipment and nodes.

Usage of other protocols shall be agreed separately (mainly in embedded and machinery controls).

6.5 Sub-netting

6.5.1 Virtual LANs

Virtual LANs shall be implemented as described in the separate Purchaser issued technical specification for OT ICT Structure, Sub-netting and Addressing.

6.5.2 IP Addresses

IP addressing shall be implemented as described in the separate Purchaser issued technical instruction for technical standard for OT ICT Structure, Sub-netting and Addressing for Operational Technology ICT.

6.6 Network Management

Network components shall have embedded RMON (Remote Monitoring) agents to enable centralized network management and diagnostics with SNMP (Simple Network Management) protocol.

Separate VLAN for network management will be set-up by Purchaser for each switch to isolate, secure and prioritize the management traffic. If the solution includes active devices; the supplier shall configure them to support the centralised network management according to instructions of Purchaser. Unmanaged network active devices shall not be used.

Only Purchaser provided network management software and tools shall be used.

7 NETWORKING

Data networks are segmented with firewall system into separate parts. The usage of firewalls or similar procedures shall be promoted for each network connected device communicating on different segment of network.

7.1 Administrative networks

The administrative part of the networks shall consist of the functions required for standard office activities, like telephony and multimedia services and connectivity to personal wireless terminals.

Mobile communication equipment shall always be communicating through access points in administrative networks.

7.2 Security networks

The security networks part of the networks consist of functions required for security and surveillance activities, where security monitoring and controls like site video surveillance, access control and intrusion detection systems are connected.

The site security related network shall be Ethernet based, using manageable “commercial off-the shelf” Ethernet equipment and software. The network system shall include provisions for using redundancy as employed in standard Ethernet applications.

There shall be physical layer redundancy between system network switches, controllers, cameras, operator stations, linking devices and other system units. The switch over to redundant path shall occur automatically if a communication failure is detected in the channel in use. Diagnostics shall be provided for all devices to indicate the health and status of the network, including the status of the redundant paths.

The network active devices shall support quality of service according to IEEE 802.1Q (Standard for Local and Metropolitan Area Networks - Bridges and Bridged Networks) and prioritization according to IEEE 802.1p (Strict Priority) with 8 priority levels.

See more about networking security aspect in separate OT-Security Policy Category “A” Sites (OT-SP_v1.1a).

7.2.1 Video systems

The video equipment, software and functions shall comply with the latest ONVIF Profile specifications to ensure compatibility.

7.2.2 Physical access control and locking systems

Communication to door environment (controllers) shall be with IP networking. Communication to door accessories (readers etc.) from the controller shall be with SIA Open Supervised Device Protocol (OSDP) latest version.

Mobile access and locking credentials shall be with NFC or Bluetooth to locks or access control readers.

7.3 Production related mission critical networks

The mission critical networks part of the networks consist of functions required for operational technologies of production.

The site utility services related network shall be Ethernet based, using manageable “commercial off-the shelf” Ethernet equipment and software. The network system shall include provisions for using redundancy as employed in standard Ethernet applications.

There shall be physical layer redundancy between system network switches, controllers, operator stations, linking devices and other system units. The switch over to redundant path shall occur automatically if a communication failure is detected in the channel in use. Diagnostics shall be provided for all devices to indicate the health and status of the network, including the status of the redundant paths.

The network active devices shall support quality of service according to IEEE 802.1Q (Standard for Local and Metropolitan Area Networks - Bridges and Bridged Networks) and prioritization according to IEEE 802.1p (Strict Priority) with 8 priority levels.

The communications between various machine and other control systems shall be done using data network facilities, Ethernet with appropriate protocols.

The system communications shall support diagnostics of the communication systems and their components.

The topology, cabling, materials and equipment of mission critical networks must be approved by Purchaser before implementation.

7.3.1 Control Networks

Control networks are part of the mission critical networks structure, where process and machinery controls are connected. Purchaser’s Technical Standard PROFINET (OT-TS_PROFINET_v1) standard and separate instructions for control networks design and installation shall be followed.

7.3.1.1 Process Controls

In cases of I/O bus or device network functionality, Profinet, EtherNet/IP or TSN with OPC UA shall be preferred as networking standard. The networks shall be constructed with manageable industrial grade active devices, capable of withstanding the environmental challenges of the installation. The active devices shall support necessary network resiliency features. The selection of applied network shall be made before design of the solutions is commenced.

The network cabling and connectors shall always be of industrial grade and fit for selected service as described in the Purchaser instructions and applicable industry standards.

7.3.1.2 Sensor and actuator networks

Sensors and actuators field network shall be realised with applicable combination of Profinet, IO-link, APL (Advanced Physical Layer) and SPE (Single Pair Ethernet). Network segments shall be sized according to specific design instructions providing adequate expansion capacity. The usage of Profibus on sensor and actuator network level shall be separately discussed and approved by Purchaser.

The topology, cabling, materials and equipment of device level field networks must be approved by Purchaser before implementation.

7.3.1.3 Conventional I/O solutions

Although serial network communications are preferred, there may be cases when the conventional I/O systems are used. The I/O units shall be individually distributable with appropriate environmental protection and shall communicate with other systems by Profibus, Profinet, EtherNet/IP or TSN with OPC UA.

The standard signals in green field (new process areas) are:

- Analogue inputs 4-20 mA, supply 24 VDC, with HART
- Analogue outputs 4-20 mA, supply 24 VDC, with HART
- Discrete inputs and outputs for field equipment 24 VDC
- Discrete inputs for motors 24 VDC (where applicable)
- Discrete outputs for motors 24 VDC (where applicable)

In the brown field the existing communication protocol will be used. The communication protocol to be decided by Purchaser in each project.

In brown field (existing process areas) standard signals are:

- Analog inputs/outputs 4 to 20 mA, supply 24 VDC, with Hart
 0 to 20 mA DC
 0 to 10 VDC
 0 to 20 VDC
- Discrete inputs/outputs 24 VDC

The impedance of analogue I/O shall be compatible with intelligent transmitters and positioners. Field instruments communication protocol (HART) shall not disturb the use of the measurement signal.

Discrete inputs and outputs shall be galvanically isolated and powered by the system.

The system shall monitor the condition of the field equipment connections and indicate faults.

7.3.1.4 Machinery and robotics controls

The networks for packaging machines and other robotics and motion controls type of applications shall be based on solutions tested with the selected device networking.

7.3.2 Building management systems networks

The building management systems networking shall be based on process control protocols (as given earlier in this document) or specific Building Automation Systems (BAS) protocols, working on Ethernet (for example Bacnet or KNX).

7.3.3 Power Distribution Systems networks

The electrical power distribution systems shall be based on protocols defined in IEC 61850 (Communication networks and systems for power utility automation) to obtain the necessary response times of < 4 ms needed for control, synchronization, protection and metering of power supply network components, mainly in the site substation but also in other parts of the power system.

8 INDUSTRIAL CONTROL NETWORK COMPONENTS

8.1 Network Switches

Control network active components shall be certified and fulfil the requirements of the selected protocols.

The switches shall support auto-negotiation (10/100/1000 Mbps, full duplex or half duplex).

The switches shall have max. 10 μ s delay time, min. 12500 bytes memory buffer per port.

The type of switching determines the line depth. If more than 5 line depth is required, switch with a “Cut Through” type of switching must be selected.

If end device require PoE/PoE+ the Switches shall be selected accordingly.

8.2 Connectors

RJ45 connectors suitable for insulation displacement method (Fast connect-type) shall be used in environmentally less demanding locations.

If RJ45 connectors are used for production related purposes, they shall be suitable for industrial use, and they shall be robust and metal enclosed.

M12 connectors (D-coding) shall be used for network cables requiring IP65 protection, i.e. for field devices in wet or vibrating environment.

The topology, cabling, materials and equipment of device level sensor buses must be approved by Purchaser before implementation.

9 COMMUNICATION LINKS

9.1 General

Asynchronous messaging type of connections shall be used instead of synchronous where applicable.

In cases where a synchronous connection is required, the links shall have a buffering capacity to cover the possible down time of the receiving end.

Complete transparency between all the information sources shall be supported by all systems.

9.2 Real time communication

9.2.1 Communication on Network Level 1

Profinet over TSN shall be used when communicating between systems on controller level.

In case Profinet interface is not available, a relevant Profinet gateway shall be used, for example:

- Modbus-TCP/Profinet
- CAN/Profinet
- Ethernet/IP /Profinet

Profinet PN/PN couplers shall be used to isolate the Profinet networks of different systems.

9.2.2 Communication on Network Level 2 and Above

9.2.2.1 OPC UA

OPC (Open Platform Communications) UA (Unified Architecture) technology shall be used to allow applications access and transfer data in and out of manufacturing systems in a consistent manner. The OPC will facilitate system integration in the existing and future heterogeneous computing environment. The latest version of OPC UA (Unified Architecture) with applicable Information Access and Industry Standard Information Models shall be implemented as preferred solution. In cases where OPC UA is not available, the classical OPC (DA, HDA, A&E) of OPC shall be used with an OPC UA gateway.

Compatibility of OPC UA products shall be verifiable by OPC Foundation certification.

Both OPC UA server and client applications shall be supported. Technical implementation of OPC UA architecture shall be approved by Purchaser before deployment.

OPC UA communication will be secured with support of OPC UA Security. Unless otherwise mutually agreed, security mode Sign and Encrypt shall be used. Management of OPC UA application instance certificates requires OPC UA Global Discovery Server (GDS) support. Purchaser will set-up the GDS service.

OPC UA communication shall use relevant standard profiles needed for the application, e.g.:

- DA Data Access
- HA History Access
- AC Alarm and Conditions

The use of the profiles shall be selected based on the communication needs and nature and will be agreed between the communicating parties.

The data models and use of OPC UA Companion Specifications (Industry Standard Information Models) and Supplier specific Information Models shall be approved by Purchaser.

Network connection through Purchaser firewall shall be used for the links between systems.

9.2.2.2 Messaging

In general OPC UA communication with applicable data models shall be used for communication between systems. In cases when information flow between applications is not continuous but happens in batches, transactional messaging can be used.

Message queuing allows for the distribution of information between systems on a network regardless of the degree of connectivity between them. It requires only an intermittent connection to make communication possible. In order to guarantee the communication, transactional messaging shall be used.

For external messaging (outside the site network) Purchaser's connectivity services shall be used.

9.2.3 Data Link Functional Control

Redundancy and link health check arrangements shall be considered and designed together with the communicating parties.

The communication links shall have watchdogs to monitor the status of the link. Link failures shall be detected and indicated by high priority alarm. Link status and maintenance software shall be included. The links shall be able to recover automatically when the connection has been re-established. In process and machinery control a reliable method of resuming a safe, controlled state of controls shall be available.

9.2.4 Responsibility of Signal Interfaces

In system implementation the Supplier shall be responsible on his side for the implementation of the communication between their system and the other systems. The Supplier shall also, without separate instructions or control, co-operate and work together with other Suppliers to ensure fully functional, working interfaces, having high availability. In case of operational faults the Supplier is responsible to prove the faultless function of their system.

The Supplier is responsible for testing of the interfaces together with the suppliers of communicating foreign systems latest during the SAT and before start of commissioning, regardless of the supplied end-point (client or server).

10 SITE ENVIRONMENT

All systems shall be designed to meet the requirements set forth by the intended location of installation. The environmental requirements are given in the application specifications located in the enquiry documentation of each application. Issues to be

handled are e.g. temperature, humidity, vibration, cleanliness, dust content and air borne chemical contamination.

In addition, security related environmental issues need to be addressed specifically for each application. Such issues are e.g. firefighting and access control, addressed also in the separate security policies.

10.1 Rooms and spaces

Rooms and spaces shall be designed and built according to guide lines given in the separate Purchaser issued technical standard for: cabinets, enclosures and rooms for operational technology ICT.

10.2 Cabinets and Enclosures

Cabinets and enclosures shall be designed and manufactured according to guide lines given in the separate Purchaser issued technical standard for: cabinets, enclosures and rooms for operational technology ICT.

11 SYSTEMS

Systems and equipment shall be marked/labelled as given in separate Purchaser issued technical instruction.

Systems and equipment shall be numbered and identified as given in separate Purchaser issued technical instruction.

System naming (hostname) must include location specific prefix matching to deployment site of the purchaser, and be unique within the site. Detailed system naming is part of detailed technical planning of the implementation.

11.1 Workstations

The HMI computing shall primarily implement in virtualized server environment.

The operator interfaces in control rooms and mobile and field connections to these systems shall be IP KVM or thin client units located in the user environment providing only the required functionality.

The control rooms work places shall be designed according to foreseen purpose. A number of displays with applicable sizes shall be grouped for each work place.

Standard commercially available field terminals, mobile workstations and pads or environmentally hardened kiosks shall be used as user interface in site areas.

11.2 Servers and virtual hosts

In general computing resources shall be implemented with a minimum of two separate hardware platforms (in separate locations) acting as a hot clustered unit providing real time system resiliency.

In general, the servers are installed in racks and cabinets in server rooms. The server cabinets shall be equipped with a networked means to enable centralized management of the servers.

The servers shall be equipped with minimum two teamed network interfaces allowing communication to system nodes through two separate channels. NIC's needed for high availability, fault tolerance and disaster recovery shall be specified separately depending on the implementation.

Servers and virtual platforms shall support on line management by Purchaser.

The hardware set-up of the servers shall be decided case by case according to need and Purchaser's equipment standards.

11.3 Back-up

In order to manage the possible hardware and software disasters off-site backups are made. Instead of distributed backup facilities the systems back-up are made to fault tolerant data network connected storage according to Purchaser established procedures. There shall be availability to optimize the procedures with automated functions, taking care of timely backup sequences and media availability with optimal use of manpower.

All engineering type of stations and servers, especially those with systems configuration and historical databases, shall be included in the automatic back-up procedures. It shall be possible to load backup agents to these units according to site standards. Purchaser instructions for manual disaster recovery of the systems and data shall be followed.

11.4 Printers

Separate hardcopy devices and printers (colour laser type) shall be connected to the a specific separate sub network. The printers shall have means to handle the print queues and provide standard printing services for all systems connected to the networks.

Special (thermal type) printers are allowed in embedded applications.

Bar code and label printers shall be according to Purchaser instructions and connected to the data network segment of the area in question.

Applications using RFID for identification shall be defined in separate specifications as applicable.

12 SOFTWARE

12.1 General

In general, open standards are preferred over proprietary solutions. If proprietary solutions are selected, this shall be clearly indicated and justified to Purchaser.

All software shall be upgradable for an updated version, especially in case of found vulnerabilities or other software bugs.

Software basic language is English and shall be expandable with additional language package according to Purchaser's specifications.

Attention shall be paid to scalability so that the systems are sufficiently powerful to handle both the current demands and are easily adaptable for future needs.

Where software or a software system is provided to be installed on shared client or server machines, the Supplier shall clearly state the hardware requirements.

Applications that make extensive use of network communications shall specify their network bandwidth requirements during both normal and upset conditions.

12.2 Dependencies and Licences

Supplier shall document all software required by their system that is supplied by third parties. Copies of licence conditions for all third party software included in Supplier's delivery shall be provided.

For propriety software a copy of proposed software licensing agreement shall be included.

License policy for each application, especially in view of connectivity shall be clearly and separately defined. System type generic licenses are not accepted in networked environment. The supplier of the systems shall provide Purchaser the information of the used software with its revisions in an exportable (XML or equal) format, to be imported to Purchaser asset management system.

12.3 Operating Systems

Purchaser's preference for server operating systems is MS Windows Server 2019 (or newer). Desktop operating systems are MS Windows 10 (or newer) based according to Purchaser's specifications. Operating system license shall be included with every workstation when delivered, unless central licensing using a KMS-server is to prefer.

For process and machinery controllers, equipment embedded control processors and other low level systems special operating systems are accepted. Hardware deliveries that include embedded software shall include the right to use the software royalty free for the lifetime of the hardware.

The implementation of the manufacturing control and other manufacturing related activities shall be based on standard MS Windows Server 2019 (or newer) product. For process and machinery control operator interface, programming, asset management, diagnostics and other office type activities also MS Windows based operating system can be used.

The applicability of Windows Active Directory and functionalities shall be separately defined in application specifications.

The usage of other operating systems shall be discussed separately.

12.4 Standard Software

Purchaser uses standard workstation package CWS in office environment (Corporate Workstation Standard) and it includes available software and software licenses for different users. Every new workstation in office environment shall be installed with CWS package according to Purchaser's instructions.

All systems and work stations in the site related services shall be hardened as given in Purchaser issued technical standard for cyber security.

12.4.1 Office Tools

The following standard office software formats shall be used:

Word processing	.docx e.g. MS Word
Spreadsheet	.xlsx e.g. MS Excel
Business graphics	.pptx e.g. MS PowerPoint
Project Management	.mpp e.g. MS Project
Portable Document Format	.pdf e.g. Adobe Acrobat

Document management according to the project standards – to be advised

12.4.2 CAD Systems

Autodesk's AutoCAD shall be used as standard CAD software.

For network and software design and documentation MS Visio with applicable applications shall be used.

12.5 Propriety Software

Suppliers of proprietary solutions need to specify:

- The development history of the product
- The current product version
- Life time expectancy and planned future releases of the product
- Current product development effort
- Support for the product
- The Supplier's policy on software upgrades and backward compatibility
- The Purchaser's rights if the product is withdrawn (e.g. access to source code / Escrow)

12.5.1 Ownership

At the conclusion of the systems implementation all rights related to custom software shall be transferred to Purchaser.

12.5.2 Preferred Implementation Technologies

12.5.2.1 General programming languages

- Java,
- C++,
- VB, (C#, VB.Net)

12.5.2.2 Control oriented programming languages,

- IEC 61131-3
- IEC 61499
- System specific block languages

12.5.2.3 Database Management Systems

- SQL Server
- MS Access (single user only)

12.5.2.4 User interfaces

- Acrobat Reader
- SAP GUI
- MS Edge

Thin Web based client interfaces should be utilized wherever possible. This is to reduce the systems administration work related to the system.

In general Purchaser shall be consulted before implementation on the application for the exact version and revision (including applicable Service Pack).

12.6 Software Deployment

Centralized application deployment and management solutions are preferred where thin web technology is not a viable solution. Supplier shall prepare set-up programs on transferrable drives for the installation of client/server applications.

13 ICT INFRASTRUCTURE

In general all ICT systems shall use Purchaser's common ICT infrastructure and infrastructure management where applicable. These includes:

- Remote access for system support/update
- Network segregation and related network security (Firewalls, Malware detection, IDS, IPS, etc.)
- Network access control and monitoring (wired/wireless)
- Virtual platform environment
- Backup services
- End Point Protection (Malware, Firewall, Whitelisting, etc.)
- Configuration Management Database for asset management
- Software and licence inventory
- Naming standards, labelling, etc...
- Common managed standard workstation

- Common managed mobile device
- Vulnerability and patch management services
- Common network services (DHCP, DNS, NTP)
- Identity and access management (including Multi Factor Authentication)
- Common directory services (Active directory)
- Data storage and collection services (“Data lakes”)
- Wireless network or Private LTE
- Security Operations Center services
- Incident, Request and Change Management -process support

The preference of system network data, security and resources management and administration is the sites Windows Active Directory (part of Purchaser’s global directories).

The site system shall be upgraded as necessary with the new systems and applications. The Supplier shall prepare their system to be included in this directory system. The applicable detailed definitions of the directory system shall be published and discussed separately.

14 TRUSTWORTHINESS

Issues and directives concerning ICT and systems trustworthiness issues shall be given in OT-Security Policy Category “A” Sites, Mondi Group IM (OT-SP_v1.1a).

Special attention shall be paid to ensuring the cyber security and other trustworthiness issues (security, privacy, safety, reliability, and resilience) of the systems and applications. The trustworthiness shall be based on applicable risk assessment procedures.

Purchaser shall issue separate instructions for implementation of physical security for ICT systems locations.

15 HARDWARE REQUIREMENTS, SCALABILITY AND COMPATIBILITY

Attention shall be paid to scalability so that the systems are sufficiently powerful to handle both the current demands and are easily adaptable for future needs. Detailed requirements are given in the systems technical specifications.

Where software or a software system is provided to be installed on shared client or server machines the Supplier shall clearly state the hardware requirements.

Systems that make extensive use of network communications shall specify their network bandwidth requirements during both normal and upset conditions.

16 USABILITY, ADMINISTRATION AND SUPPORT

The Supplier shall describe the administrative and support tasks required to keep the systems operational. In addition they shall describe the skills required of administrative and support staff to perform those tasks.

16.1 Availability, Performance, Monitoring and Management

The availability and the performance figures and verification of each system shall be specified in the system enquiries and further in the delivery contracts. These figures shall be used to verify the performance and faultless operation of the system and/or any part of it during the guarantee period.

The application performance shall be monitored and reported with applicable tools (network management, intrusion detection, cyber security monitoring etc) provided by Purchaser.

In general all system nodes shall support SNMP for network management and availability and performance monitoring. The network monitoring is used to monitor network performance, detect and report problems and collect information for problem solving.

SNMP agents shall be located in network elements to report to and respond to requests of the management stations in the Site network. Permanently installed network analysers shall be used to verify the long term availability and performance of network connected equipment and applications.

If the systems or some parts of the systems do not support the SNMP and standard data network remote monitoring, the Supplier shall agree with Purchaser the methods of remote availability and performance monitoring.

17 SYSTEMS DESIGN AND IMPLEMENTATION

17.1 Engineering

The required engineering within the Supplier's responsibility shall be according to good standards of engineering practice.

17.2 Hardware Engineering

The systems documentation shall include:

- Design drawings and documents for hardware including overall systems structures, hardware specifications and layouts with unit identification and reserve place indications etc.
- Protocols and descriptions of trustworthiness risk assessment and abuse testing
- Design and drawings of AC and DC power distribution of all required equipment with power requirements for the site UPS. Before installation, the drawings must be approved by Purchaser.
- Design and drawings of earthing for each system and requirements for earthing impedance.
- Design and drawings for cabling between different systems and cabinets including details of cable termination.
- Cable list and termination drawings for installation.
- Certified dimensional drawings for all units of equipment included in delivery.
- Necessary documentation for installation, including any special requirements.

The exact document delivery and time schedule shall be separately agreed according to project scope and time schedules.

17.3 Software Engineering

17.3.1 General

Separately issued OT-Security Policy Category “A” Sites, Mondi Group IM (OT-SP_v1.1a).shall be considered and followed in the software delivery and engineering activities.

17.3.2 Specification

All software systems shall be fully specified before implementation commences. The use of text based descriptions, diagrams, drawings, prototypes etc. shall be agreed on a case-by-case basis.

The specification shall be validated and approved prior to commencing implementation of the software.

17.3.3 Engineering

Before commencing engineering of the software Supplier shall have an approved project plan. This shall include a project schedule, quality plan, manning schedule, etc.

In the Supplier’s quality plan it should be stated what methods they intend to use to ensure that their software conforms to the specification.

The Supplier shall complete their own testing before any formal acceptance testing commences (Factory Acceptance Test for instance).

17.3.4 Documentation

Custom software shall be supplied with documentation in appropriate languages for each of the following three purposes:

User documentation (Mill site’s native language).

Documentation shall enable the end users of the system to use it and perform daily services effectively. The basic user graphical interface for monitoring and controls shall be in site language, additional system messages can be in English.

Administration and Maintenance Documentation (English).

Instructions shall be used for systems administrators to install the system and maintain it in operation.

Program Documentation (English).

The programs shall be sufficiently documented to enable Purchaser or third parties to understand and then modify the program code, where applicable. This will generally require documentation external to the source code and comments.