USER REQUIREMENTS SPECIFICATION

DATA INTEGRATION MODEL FOR A PACKAGING LINE

UNIT DOSE VIALS (UDV) MONODOSE STERILE

This document has been prepared by the "Connected Machines" workgroup of GAMP Italia COP, according to the document structure proposed by the GAMP 5 Guideline (Appendix D1 - "User Requirements") .

*This document contains both guidelines for completing the document (using **a red coloured style**) and a set of practical examples that is the real body of the document. Sentences extracted from GAMP 5 Guideline and other GAMP reference documents have been included in the document with **a blue coloured style** as an additional tool to properly complete the template.*

This document has been developed as much as possible independently of a specific solution.

GAMP 5 - Appendix D1 - Paragraph 3.1 – General Guidelines

A URS defines, clearly and precisely, what the regulated company requires the system to do. It should be driven by the business process needs. Requirements may be developed independently of a specific solution prior to selection, e.g. for Category 4 and Category 5 systems. There may be a limited number of suppliers or a preferred supplier for some systems, in which case requirements may be based on the available solution. This is particularly relevant to many Category 3 systems. Such a decision should be based on risk, complexity, and novelty. In such cases requirements related to patient safety, product quality, and data integrity still should be specified. ...

Acknowledgment

This URS document template is the outcome of work done by the members of Connected Machines Working Group, part of GAMP Italy Community of Practice. This documents does not reflect the view of any one individual or company.

Document Authors - Reviewers

Agazzi Pier Luigi - Adeodata
Bellentani Marco - MG2 S.r.l.
Bosisio Paolo - PHASE
Casagranda Luca - e-PHARMA
Centin Gabriele - AKKA Italia
Chiarabaglio Andrea - Recordati
Cupone Giovanna - Patheon - Thermo Fisher Scientific
De Caris Sandro – GAMP Italia Chair - Consultant
Ghelfi Massimo - Consultant
Iannuzzi Giovanna – Ympronta S.r.l.
Lenoci Cosimo - Angelini Pharma S.p.A.
Menin Giuseppe - COPA-DATA
Mihailisin Igor - Consultant
Minardi Marco - IMA S.p.A.
Sala Andrea - DELPHARM Milano S.r.l.
Scognamiglio Fabio - Angelini Pharma S.p.A.
Selvatici Stefano – Marchesini Group
Silvaggi Vittorio - Patheon - Thermo Fisher Scientific
Testino Mario - Servitecno
Tomaiuolo Michele - Chiesi Farmaceutici
Vanti Pier Luigi – IMA S.p.A.
Velicogna Sigfrido - IBSA Farmaceutici Italia Srl

For more information or clarifications you can contact the Workgroup Co-ordinators:
Marco Bellentani – MG2 S.r.l. – mbellentani@mg2.it
Giuseppe Menin - COPA-DATA - giuseppe.menin@copadata.com

User Approval Signatures

This document has been reviewed and approved by <Company Name> to be used by Supplier.

Role	Name	Date	Signature
Author(s)			
Engineering	<Name>		
Manufacturing	<Name>		
Reviewer(s)			
Engineering	<Name>		
Manufacturing	<Name>		
Quality Assurance	<Name>		
Approver(s)			
Engineering Manager	<Name>		
Manufacturing Manager	<Name>		
Quality Assurance Manager	<Name>		

Complete and adjust the table with all the roles involved in the process of authoring, reviewing and approving of the document.

Table of Contents

1 INTRODUCTION 7
1.1 PURPOSE 7
1.2 CONTRACTUAL STATUS 9
1.3 LIMITATIONS 9
1.4 RELATIONSHIP TO OTHER DOCUMENTS 10
1.5 TERMS 11
2 OVERVIEW 12
2.1 REFERENCE TO DIGITAL PLANT MATURITY MODEL DPMM BY BIOPHORUM 13
2.2 GENERAL REQUIREMENTS AND EXPECTED BENEFITS 13
2.2.1 Easy Integration of machines. 14
2.2.2 Line operation from a centralised workstation. 14
2.2.3 Line based Recipe Management 14
2.2.4 Line based Data Storage 14
2.2.5 Centralised User Management. 15
2.2.6 Line based Reporting. 15
3 MACHINE/LINE CONNECTIVITY REQUIREMENTS 16
3.1 REGULATORY REQUIREMENTS 16
3.1.1 System Regulatory Requirements 16
3.1.2 Electronic Records Requirements 22
3.1.3 Electronic Signatures Requirements 24
3.1.4 Data Integrity Requirements 26
3.2 GENERAL REQUIREMENTS 28
3.2.1 Recipes and Configuration Management 31
3.2.2 Audit Trail management 32
3.2.3 Batch/Lot operations 33
3.2.4 Data Integrity 34
3.2.5 Operational Efficiency 36
3.2.6 Critical GxP parameters and process data monitoring 36
3.2.7 Data Analytics 37
3.2.8 Exception Handling 39
3.2.9 Electronic Batch Record 41
3.2.10 User Management and Access Control 42
3.2.11 Cyber Security 44
3.2.12 Remote control 46
4 DETAILED REQUIREMENTS FOR UNIT DOSE VIALS (UDV) MONODOSE STERILE PACKAGING LINE 47
4.1 SYSTEM / PROJECT OVERVIEW 47
4.2 APPLICABLE STANDARDS 48
4.2.1 PACKML – ISA TR 88.00.02 48
4.2.2 OPC-UA 51
4.3 FUNCTIONALITIES OF A LINE EXECUTION SYSTEM 52
4.3.1 Recipe management 53
4.3.2 Opening the Batch 53
4.3.3 During batch execution 56
4.3.4 Batch Closing 57
4.3.5 Long-term data management 60
4.4 UNIT DOSE VIALS (UDV) PACKAGING LINE PARAMETERS 60
4.4.1 Blow Fill Seal 60
4.4.2 Leak Detector 65
4.4.3 Check weigher 66

4.4.4 Strip printing and vision system 66
4.4.5 Storage buffer 67
4.4.6 Overwrapping machine with printing and vision system 68
4.4.7 Cartoning machine with printing and vision system 69
4.4.8 Boxes check weigher 70
4.4.9 Labeller (label printing and vision system) 71
4.4.10 Cartopalleting machine with printing and vision system 72

5 OPERATIONAL REQUIREMENTS 74

6 CONSTRAINTS 75

7 LIFE-CYCLE REQUIREMENTS 76

8 GLOSSARY 77

9 ATTACHMENTS 78

Template Revision History

This paragraph relates to the Template; it is therefore to be deleted when a new document is generated using this Template.

Only the Document Revision History should remain in the actual document.

Rev.	App. Date	Written by	Revised by	Approved by	Revision Summary
01	10/05/2022	GAMP Italia Connected Machines WG	GAMP Italia Connected Machines WG	GAMP Italia Connected Machines WG	Initial Release

Document Revision History

Rev.	App. Date	Written by	Revised by	Approved by	Revision Summary
01	-	-	---	-	Initial Release

1 INTRODUCTION

GAMP 5 - Appendix D1 - Paragraph 3.1 – Introduction

The introduction will provide information on:

- *who produced the document, under what authority, and for what purpose*
- *the contractual status of the document (if applicable), e.g.,*
  - *custom development*
  - *outsourcing*
- *relationship to other documents (e.g., Business Process Definition, Request for Proposal (RFP))*

The URS is a document that has the purpose to define the expected system performances and is the basis for the design and verification phases of the equipment.

This document should be provided starting from the request for quotation and however it must be provided in a final version when the contract is defined.

The URS must be kept up-to-date for the entire equipment development life-cycle as it is the input for the subsequent phases.

In case of complex changes required after acceptance of the system, a new URS document focused on the changes required should be issued.

This document was generated under the authority of the <Company Name> Company for the purpose of specifying the user requirement of a unit dose vial filling and packaging line.

Sections 1 and 2 of this document are only explanatory and are not intended to be object of a verification activity at later stages of the system delivery.

Only uniquely coded requirements of sections 3 and 4 will be object of a verification activities.

1.1 Purpose

GAMP 5 - Appendix D1 - Paragraph 1 - Introduction

... The extent and detail of requirements should be commensurate with risk, complexity, and novelty, and should be sufficient to support subsequent risk analysis, specification, configuration/design, and verification as required. The results of any existing studies, such as business need analysis, may assist with determining the extent and detail of requirements. ...

The User Requirements Specification (URS) is provided to aid the user through the major components, variables and options necessary to procure a functional "**Monodose Sterile Line - Unit Dose Vials (UDV)",** that meets the user's needs in the most cost-effective method possible.

The document defines a minimum set of requirements for packaging line machines regarding vertical data integration with specific IT services.

In this case, the line is installed in a company that has an ERP system, but has neither a MES/EBR system nor a plant historian.

For this reason, services like, line management, data storage, reporting and changeover support are required at line level.

The following image shows the general scheme of the desired communication level for the line and the systems connected to it. Therefore, the main purpose in the realization of this line is to allow all the systems involved to make the generated data available and to draw those necessary for a better usability, efficiency and compliance of the production process.

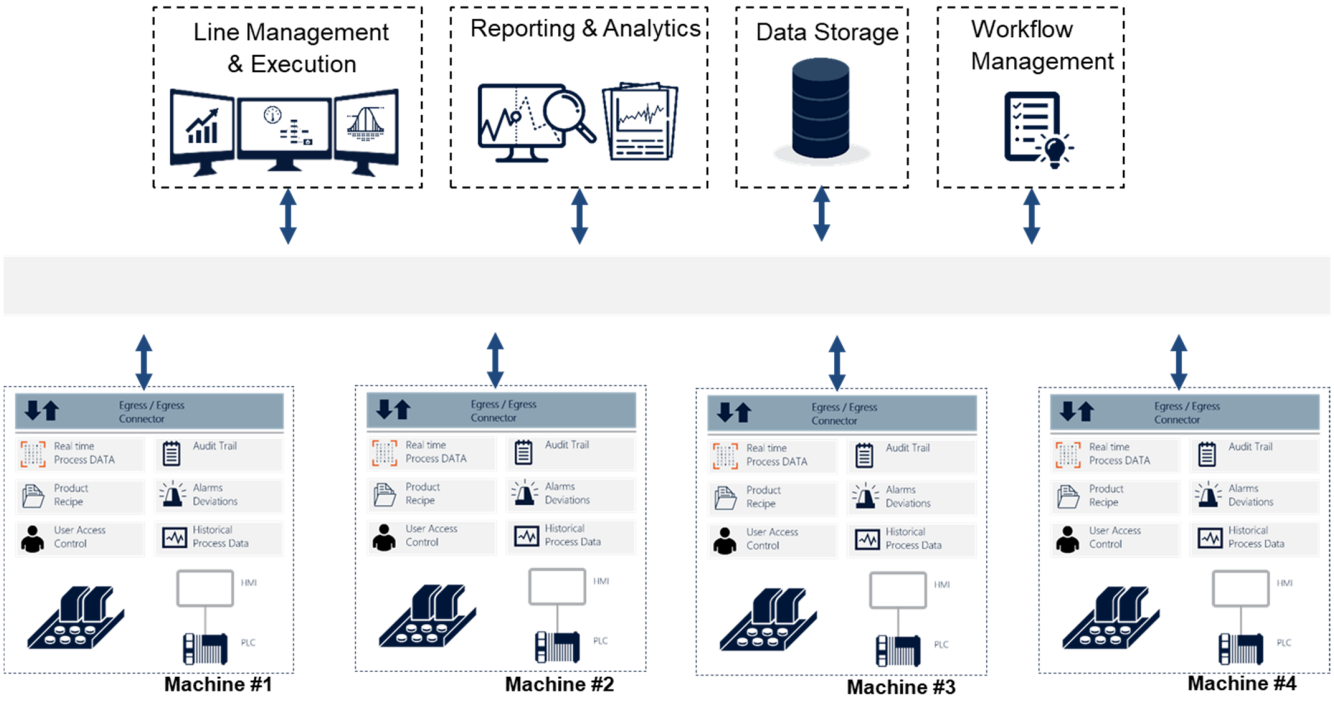


Fig.1 – General overview of Machines and Line Level software services.

The URS is then provided to the Supplier as an input for the quotation, design, construction, commissioning and validation of the system.

1.2 Contractual status

This URS will be recognized as an integral part of the procurement agreement with the selected system vendor. The system supplier or vendor will abide by the information and conditions set forth by this document as well as the standard purchasing term and conditions of the <Company Name> Company.

1.3 Limitations

Insert possible limitations to the use of the document.

Example: URS are confidential and property of the "<Company Name>" . The use, the copy and the distribution of the document are not permitted.

1.4 Relationship to other documents

The present URS can be complemented with other documents such as specific URS for the connected equipment.

Include possible reference to external Risk Assessment documents (if existing) that formalizes the ratio of criticality levels of specific requirements indicated in the URS document.

As an example we provide a generic reference contents to be used for the possible external documents to which punctually references may follow in the document.

INSERT HERE THE REFERENCE TO THE IDENTIFIED DOCUMENT(S)

1.5 Terms

Verify and integrate the definition of terms used in the document and their meaning.
Insert possible further indications the help the proper interpretation of the document.

Where statements in the specification include the words “must”, “shall”, "is to" or “will”, it indicates that compliance with the item is regarded as mandatory. Where such recommendations cannot be implemented, the Supplier must notify the User.

Where the word “should” or “may” is used, the statement is a recommendation for guidance and adoption as good practice. It is accepted that an alternative may be more appropriate, however consultation with User is still required.

2 OVERVIEW

GAMP 5 - Appendix D1 - Paragraph 3.2 - Overview

An overview of the system will be provided, explaining why it is required, and what is required of the system. The following will be considered:

- *background: describes the overall goal of the system in context of the present and desired state*
- *scope:*
  - what portion of the long-term vision the current system will address
  - system limits and boundaries: what business process or portion of a business process is being automated
  - key objectives and benefits
  - applicable GxP requirements
  - other applicable regulations

Provide a high level general description of the system in order to anticipate the detailed requirements that will be included in the following sections.

This paragraph does not have to contain specific requirements.

This URS document has the main purpose of detailing the communication methodology of the line with all interconnected systems, delegating all non-pertinent aspects to detailed documents written by the competent departments.

The following requirements indicate the details necessary to define the desired data connection between the machines in the line and the line services in order to implement a complete system that can lead to an automated process able to create a flow of data on multiple levels, regardless of the type of machines and systems.

2.1 Reference to Digital Plant Maturity Model DPMM by BioPhorum

A few years ago, the international association Biophorum proposed a five-level model to try to assess the level of digital maturity of a pharmaceutical plant.
From an initial analysis conducted by Biophorum, most pharmaceutical companies are at a maturity level between 1 (Pre-Digital plant) and 2 (Digital Silos).

The aim of this document is to ensure that this line achieves the functionalities required by level 3 of the DPMM (Connected plant). In other words, a situation where the machines composing the line are permanently connected to higher level software services, both for reasons of regulatory compliance and to improve operational efficiency.

Level 1 Pre-digital Plant	Level 2 Digital Silos	Level 3 Connected Plant	Level 4 Predictive Plant	Level 5 Adaptive Plant
Primarily Paper-based processes Predominately manual processing. Low level of automation. Basic PLC controls. Applications are stand-alone with minimal or no integration.	"Islands of automation" Some manual processes. Batch records may be semi-electronic or "paper on glass" Local batch-recipe system interfaced to PLCs Site-specific systems; limited integration across functional silos Analytics on demand, "why did it happen?" high manual effort	Vertical Integration ERP, LES, MES and Automation layer are fully integrated to support digitized business processes. Full Electronic Batch record with review by exception. Standard application platform adopted across plant network Islands of real-time Process analytics Analytics semi-automated; "where else can it happen?"	Enterprise Integration - internal integration of plant to value chain Integration of Product Development and Manufacturing (PLM with Recipe Management) End-to-end supply chain visibility with limited external collaborations (suppliers / CMOs). Online/At-line quality testing with Real Time Release. Simulation used for process modeling and improvements Integrated Real-time Process analytics and simulation Proactive analytics across plant and internal value chain; "what can happen and when?"	Full end-to-end value-chain integration from suppliers to patients IT supports multiple manufacturing modes: Modular, mobile, continuous... "Plug-n-play everything" from an instrument to a production scale or a CMO Zero system down-time (including upgrades) – continuous evolution. In-line, real-time, continuous, closed loop, process verification and control with automated real-time quality release Self-aware, continuously adaptive, "Autonomous" plant; exception conditions handled by remote experts Pervasive use of adaptive analytics and Self/ Machine learning across value chain.

2.2 General requirements and expected benefits

In order to reach level 3 according to the DPMM, certain general requirements are required of the line as a whole.

Even if the line consists of several machines, the intention here is to define what is required by a machine to be integrated with a centralised system for managing the line. A system that we will call Line Execution System (LES).

In the following paragraph we provide an overview of LES general features:

2.2.1 Easy Integration of machines.

Communication between machines and higher services must be carried out using universally accepted, vendor-independent standards. In this case, it is considered appropriate to use OPC UA as the communication language and PackML (ISA TR88.00.02) as the mode of representation of machine states and description of information.
The machines must be prepared to support these standards and must be able to work in both 'stand-alone' and 'connected' modes.

2.2.2 Line operation from a centralised workstation.

From the centralised workstation in the LES level, the operator must be able to manage the entire batch to be produced. This starts from the change over phase, receiving information on the operations to be carried out to prepare the line, to the opening of the batch, to the selection of recipes in the various machines, to the monitoring of production, to the display of alarms and Audit Trail, to the final report at the end of production.
When the machine is in 'connected' mode the operator does not have to walk back and forth across the line to find out what is going on.

2.2.3 Line based Recipe Management.

The recipes represent the sets of various machines to produce a given product. Each machine has its own local recipe management. The line level shall implement a "line recipe" which includes a reference to the recipe to be loaded in each machine for a given product. The line recipe management system has to implement status and versioning in order to achieve an appropriate approval workflow. This simplifies the batch opening phase and reduce errors as each product has a unique reference to the sets on each machine.

2.2.4 Line based Data Storage.

During production, each machine produces data that needs to be stored for compliance or simple business reasons.
This historical data can be grouped into:

- Process variables: time series data

- Alarms: statefull events
- Events: stateless events

Historical data must be stored in a single repository at line level. This simplifies the management of backup/restore activities and allows simplified and consistent access to information by visualisation and reporting services.
The data storage can be physically installed in-line or on a corporate data centre.

2.2.5 Centralised User Management.

User management must be common between the machines and the LES system so that the same user can operate at both machine and line level, also ensuring a consistent audit trail. The various systems must therefore be integrated with Domain Servers such as Microsoft Active Directory.

2.2.6 Line based Reporting.

There must be a service at line level capable of generating reports in readable format, both on screen and printable.
The reports must satisfy:

- End of batch reports highlighting exceptions to implement Review by Exceptions.
- Statistical Process Control as an evidence of process quality level and to provide tools for improving product quality.
- Performance indicators such as OEE to provide a simplified representation of line performance.
- Regulatory requirements (see paragraph 3.1 for details)

3 MACHINE/LINE CONNECTIVITY REQUIREMENTS

3.1 Regulatory Requirements

The requirements of procedural or otherwise non-functional type are identified with the letter P and are not to be implemented at system level (management is needed at procedural level, such as the creation of a SOP). The letter F identifies a functional requirement.

In the column "APPL." the requirements finds an application on this level:

- M/C CON = Machine Connectors
- LES = Line Execution System

If the requirement is not applicable to both columns, it is marked with grey color but left as a reference as it is GMP relevant.

3.1.1 System Regulatory Requirements

Below is the list of regulatory requirements that shall be satisfied by the system.
All the following requirements are considered necessary and GMP relevant (non-applicable requirements should be identified and justified (and reported in the Traceability Matrix).
In some cases a generic reference to Data Integrity Guidelines is provided referencing current guidelines from MHRA, GAMP and PIC/S PI 041-1.

REQUIREMENT CODE	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	21 CFR PART 211; PART 11	EU GMP VOL4; ANNEX 11	P/F	APPL.	
						M/C CON	LES
UR.R001	**Validation**	The applications should be validated.	211.68 (a) 11.10 (a)	Vol.4 §4.1 Annex 11 principles	P	X	X
UR.R002	**Qualification**	IT infrastructures should be qualified.	N/A	Annex 11 principles	P		
UR.R003	**Risk Management (Life Cycle)**	Risk management should be applied throughout the life cycle of the computer system, taking into account patient safety, data integrity and product quality.	N/A	Annex 11 §1	P		

REQUIREMENT CODE	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	21 CFR PART 211; PART 11	EU GMP VOL4; ANNEX 11	P/F	APPL.	
						M/C CON	LES
UR.R004	**Risk assessment**	Decisions about the extent of validation and data integrity should be based on a justified and documented risks assessment (Risk Management) of the computer system. Standards, protocols, acceptance criteria, procedures and records should be based on risk assessment.	211.68 (a)	Vol.4 §4.1 Annex 11 §1, §4.1, §4.2	P	X	X
UR.R005	**Training**	It should be ensured and documented the proper training of the following figures about system use: • System Users; • System administrators; • System Maintenance personnel.	211.25 (a); 11.10 (i)	Annex 11 §2	P		X
UR.R006	**Suppliers and internal IT departments Responsibility**	Systems or system related services suppliers (installation, configuration, data processing, etc.) should have formal agreements (contracts) which clearly established responsibilities. The internal IT departments are similarly regarded.	N/A	Annex 11 §3.1	P		
UR.R007	**Supplier assessment**	Each supplier should be properly evaluated. The procedures for verifying the supplier competence and reliability will be based on risk analysis.	N/A	Annex 11 §3.2, §4.5	P	X	X
UR.R008	**Off-the-shelf products**	Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.	N/A	Annex 11 §3.3	P	X	X
UR.R009	**Suppliers quality system and audit documentation**	Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request	N/A	Annex 11 §3.4	P	X	X
UR.R010	**System Change Control and Configuration Management**	Changes to the computerized system, including those made to system configurations, should only be implemented according to specific procedures of Change Control / Configuration Management. Such procedures shall allow to know the changes over time in the system (hardware, software, documentation) and system configuration.	11.10 (k)(2)	Annex 11 §10	P	X	X
UR.R011	**Protection of computerized system configuration settings**	Computerized system configuration settings should be defined, tested as part of computer system validation, and protected from unauthorized access	N/A	Annex 11 §10	P/F	X	X

REQUIREMENT CODE	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	21 CFR PART 211; PART 11	EU GMP VOL4; ANNEX 11	P/F	APPL.	
						M/C CON	LES
UR.R012	**Inventory**	An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.	N/A	Annex 11 §4.3	P		X
UR.R013	**System documentation Management**	There should be a procedure defining the methods of distribution, access and use of the system documentation throughout the entire life cycle of the system.	11.10 (k)(1)	Vol.4 §4.2	P	X	X
UR.R014	**User requirements**	User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle.	N/A	Annex 11 §4.4	P	X	X
UR.R015	**Bespoke system**	For the validation of bespoke or customised computerised systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system.	211.68 (a)	Annex 11 §4.6	P	X	X
UR.R016	**Validation tests**	It should be documented and evaluated: • methods and conditions of test execution; • system parameters limits, • data limits and error handling; • automatic testing tools; • Test execution environment.	N/A	Annex 11 §4.7	P	X	X
UR.R017	**Data migration**	If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.	N/A	Annex 11 §4.8	F		
UR.R018	**Univocal Temporal Reference**	The time reference should be univocal for each system component.	11.10(e), 11.50 (a)(2)	Annex 11 §14.c	F	X	X
UR.R019	**Access control**	The system should allow access only to authorized users. The amount of security checks depends on the criticality of the system (pass cards, ID and password, biometric systems, encrypted documents, etc.)	211.68 (b); 11.10 (d); 11.30	Annex 11 §12.1; §12.2	P/F	X	X

REQUIREMENT CODE	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	21 CFR PART 211; PART 11	EU GMP VOL4; ANNEX 11	P/F	APPL.	
						M/C CON	LES
UR.R020	**System administrator access**	System administrator access should be restricted to the minimum number of personnel possible, taking account of the size and nature of the regulated company. Personnel with system administrator access should log in under unique logins that allow actions in the audit trail(s) to be attributed to a specific individual. The generic system administrator account should not be available for use. (Data Integrity Guidelines)	N/A	N/A	P	X	X
UR.R021	**Changes performed under system administrator access**	Critical changes with data integrity implications (e.g., system access changes, configuration changes, data movement, data deletion etc.) performed under system administrator access should be visible to, and approved within, the quality system. (Data Integrity Guidelines)	N/A	N/A	F	X	X
UR.R022	**Access authorizations recording**	Creating, changing and deleting access authorizations should be recorded.	N/A	Annex 11 §12.3	P/F	X	X
UR.R023	**System access records review**	System access records should be periodically reviewed based upon the criticality of the process supported by the computerized system. (Data Integrity Guidelines)	N/A	N/A	P	X	X
UR.R024	**System Access**	Access to the system should be made using an account made by identification code and password. Pass through technologies such as single sign on that leverage earlier user authentication are acceptable.	11.10 (g)	Annex 11 §12.1	F	X	X
UR.R025	**Password uniqueness**	The system should not allow the creation of two identical combinations of identification code / password.	11.300 (a)	N/A	F	X	X
UR.R026	**Password Management**	• The system should force the user to change passwords after a predetermined period of time according to the policy in force. • The system should allow the user to change his password at any time, regardless of the validity period. • The system should be capable to reset the password at any time, regardless of the period of validity.	11.300 (b) Part 11 - Preamble §131	Annex 11 §12.1	F	X	X

REQUIREMENT CODE	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	21 CFR PART 211; PART 11	EU GMP VOL4; ANNEX 11	P/F	APPL.	
						M/C CON	LES
UR.R027	**User access manual disabling**	The system should generate a log where all access, including failed login attempts, are recorded. It should be possible to disable a user access. User access can be reinstated only by the system administrator.	11.300 (c) Part 11 - Preamble §135	Annex 11 §12.1,2	F	X	X
UR.R028	**User access automatic disabling**	After a predetermined number of consecutive errors entering the password, the system should disable user access. User access can be reinstated only by the system administrator.	11.300 (c) Part 11 - Preamble §135	Annex 11 §12.1,2	F	X	X
UR.R029	**Unauthorized access management**	The system should be able to detect, block and report promptly to the system administrator all unauthorized access attempts.	211.68 (b); 11.300 (d)	Annex 11 §12.1,2,3	P/F	X	X
UR.R030	**Auto Log Off**	During a system login session, the system should provide an automatic log off mechanism after a predetermined period of inactivity	Part 11 - Preamble §124	N/A	F	X	X
UR.R031	**Functional profiles**	The system should allow the assignment of functional profiles with different access levels and different privileges, in order to ensure that each user can only perform the actions allowed by their profile.	11.10 (g)	N/A	P/F	X	X
UR.R032	**Data Source Control**	The system should be able to perform device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	11.10 (h)	N/A	F	X	X
UR.R033	**Operational Check**	During the course of critical operational sequences (e.g. Data insertion / modification sequence), the system should ensure that the individual steps of the process are carried out according to the defined order and should disallow non-permitted sequencing of GxP steps and events.	11.10 (f)	N/A	F	X	X
UR.R034	**Accuracy Control**	The entry of critical data in the system shall require an additional check on data accuracy that will be performed by a second operator or by validated electronic tools. The criticality and the potential consequences of incorrect or improperly entered data into the system should be examined in the risk management.	211.68 (b)	Annex 11 §6	P/F	X	X

REQUIREMENT CODE	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	21 CFR PART 211; PART 11	EU GMP VOL4; ANNEX 11	P/F	APPL.	
						M/C CON	LES
UR.R035	**Users responsibilities**	The responsibilities of each user should be clearly defined according to the assigned functional profile, including the responsibility arising from the use of an electronic signature.	11.10 (j)	Annex 11 §2	P	X	X
UR.R036	**Batch release**	• The system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. QPs should be clearly identified and recorded by the system. • Certification and batch release should be performed using an electronic signature. • For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry.	211.68 (b) 211.101 (c)(1)	Vol.4 §4.20 (c); Annex 11 §15 Annex 11 §8.2	P	NA	X
UR.R037	**Error Handling**	All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.	N/A	Annex 11 §13	P	NA	X
UR.R038	**Business continuity**	For the availability of computerised system supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.	11.10 (c)	Annex 11 §16, §1	P/F	X	X
UR.R039	**Access Devices**	Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	211.68 (b); 11.300 (e)	Annex 11 §12.1 §12.2	P	X	X
UR.R040	**Periodic review**	Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP.	211.68 (a)	Annex 11 §11	P		

3.1.2 Electronic Records Requirements

Regulatory requirements to be met by the system about Electronic Records management are shown below. Electronic Record is defined as: "Any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system".
Where applicable, these requirements should be met for each type of electronic record that falls within the 21 CFR Part 11 (section 4.1) scope.
The retention period of the Electronic Record shall be at least XX years.

REQUIREMENT CODE	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	21 CFR PART 211; PART 11	EU GMP VOL4; ANNEX 11	P/F	APPL. (Y/N)	
						M/C CON	LES
UR.R041	**Alteration of Electronic Records**	The system should be able to detect invalid or altered records.	11.10 (a)	N/A	F	X	X
UR.R042	**Electronic Records copies**	The system should allow to generate accurate and complete copies of all data contained in electronic records. Copies should be produced both in readable (on-screen display, print) and in a standard electronic format (e.g.. ASCII, PDF).	211.68 (b); 11.10 (b)	Vol.4 §4.2 Annex 11 § 7.1, §8.1	F	X	X
UR.R043	**Electronic Records Inspection**	Electronic records should be made available in case of inspections.	211.180 (c); 11.10 (b)	N/A	P	X	X
UR.R044	**Secure Data Archiving**	The system should allow to archive and preserve electronic records, including relevant metadata, in a secure way, protected from physical and electronic damage, for as long as required by regulations. Archiving should allow the fast restoration of data. The destruction of data may be allowed only after the end of the retention period required by the regulations.	211.180 (a), (b); 211.68 (b); 11.10 (c)	Vol.4 §4.1, §4.10 Annex 11 §7.1	P/F	X	X
UR.R045	**Interfaces**	Computerized systems that exchange data with other systems should include appropriate incorporated controls, (built-in checks), to ensure the correct and secure data entering, in order to minimize the risks.	N/A	Annex 11 §5	F	X	X
UR.R046	**Back up**	There should be a procedure for the backup management. The integrity and accuracy of backups, and the ability to restore them, should be checked during validation and monitored periodically.	211.68 (b) 211.180 (d) 11.10 (c)	Annex 11 §7.2	P/F	X	X

REQUIREMENT CODE	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	21 CFR PART 211; PART 11	EU GMP VOL4; ANNEX 11	P/F	APPL. (Y/N)	
						M/C CON	LES
UR.R047	**Audit trail**	For each operation of creating, modifying or deleting an electronic record the system should automatically generate an audit trail in which all the information related to user activity are recorded.	11.10 (e)	Annex 11 § 9	F	X	X
UR.R048	**Contents of an Audit Trail**	Each audit trail generated by the system should contain the following information: • User ID; • Date and time of each electronic record transaction carried out; • Type of operation performed (creation, modification or deletion). In case of change of an electronic record the audit trail, generated simultaneously by the system, should contain information on: • Inserted, modified or deleted data (parameters, size); • data status / value before and after the transaction execution; • reason for change or deletion of data with GMP impact.	11.10 (e)	Vol.4 §4.9 Annex 11 §9 Annex 11 §12.4	F	X	X
UR.R049	**Retention of Audit Trails**	Audit trails should be retained for the whole period of record retention of the associated records, as mandated by the GMP.	11.10 (e)	Annex 11 §9	P	X	X
UR.R050	**Audit Trail integrity**	The system should not allow editing the contents of the audit trail.	11.10 (e)	N/A	F	X	X
UR.R051	**Audit Trail copies**	The system should allow to create copies of the audit trails, both in readable form (on-screen display, print) and in standard electronic format.	211.68 (b); 11.10 (e)	Annex 11 §9	F	X	X
UR.R052	**Audit Trail Inspection**	Audit trails should be available in case of inspections, during the entire retention period of the records.	11.10 (e)	N/A	P	X	X
UR.R053	**Audit Trail review**	Audit trails should be regularly reviewed. The system should enable review of audit trails that capture changes to critical data, e.g., as part of the review of their associated records Based upon risk, procedures should be established to review audit trails with each critical record, and before final approval of the record.	N/A	Annex 11 §9	P/F	X	X

3.1.3 Electronic Signatures Requirements

Most technical requirements are guaranteed by the supplier of the system, as documented in the <SUPPLIER> White Paper, and do not need further functional verifications. Formal validation may be required in the future, in case <USER> decide to use the electronic signatures for regulatory purposes, in place of handwritten signatures.
Electronic Signature is defined as: "Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature".
Procedural requirements do not need formal verification, not being applicable to the system.

REQUIREMENT CODE	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	21 CFR PART 211; PART 11	EU GMP VOL4; ANNEX 11	P/F	APPL. (Y/N)	
						M/C CON	LES
UR.R054	**User identities**	The identity of each user assigned to an electronic signature should be verified by a specific procedure, prior to the electronic signature assignment.	11.100 (b)	N/A	P	X	X
UR.R055	**Electronic signatures - handwritten signatures equivalence**	Within the system electronic signatures should be considered fully equivalent to handwritten signatures. The consequences of misuse or falsification should be documented.	11.2 (a), (b) 11.10 (j)	Annex 11 §14.a	P		
UR.R056	**Certification to FDA**	It is required to certify to FDA, with a paper document signed with a handwritten signature, that electronic signatures are considered fully equivalent to handwritten signatures within the system, before using electronic signatures.	11.100 (c) 11.100 (c)(1)	N/A	P		
UR.R057	**Electronic records signature**	Each record signed electronically should contain the following information: • Full name of the signer; • Date and time of signing; • Meaning / reason associated with the signature (Revision, approval, etc.).	11.50 (a) (1,2,3) 11.50 (b)	Annex 11 §14.c	F	X	X
UR.R058	**Electronic signature manifestations**	In case of on-screen display or print of an electronically signed record, all the information about the electronic signature shall be included and visible or printed.	11.50 (b)	N/A	F	X	X
UR.R059	**Electronic Record – Electronic Signature link**	The system shall ensure that electronic signatures cannot be excised, copied, or otherwise transferred to falsify an associated electronic record [by ordinary means].	11.70	Annex 11 §14.b	F	X	X
UR.R060	**Electronic Record – Handwritten Signature link**	A procedure should be in place to ensure that the linkage of handwritten signatures to electronic records is maintained throughout the retention period.	11.70	Annex 11 §14.b	P	X	X

REQUIREMENT CODE	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	21 CFR PART 211; PART 11	EU GMP VOL4; ANNEX 11	P/F	APPL. (Y/N)	
						M/CON	LES
UR.R061	**Electronic signature uniqueness**	The system should ensure that an electronic signature is assigned to a single user and cannot be reused or reassigned to any other user.	11.100 (a)	N/A	F	X	X
UR.R062	**Electronic signature execution**	The system shall allow the electronic signature execution in at least one of the following ways: • Electronic signature based on biometrics. 21 CFR Part 11.3 (b) (3) • Non-biometric electronic signature. 21 CFR Part 11.3 (b) (5)	11.200 (a),(b)	N/A	P	X	X
UR.R063	**Electronic signature components**	A non-biometric electronic signature shall consist of at least two distinct identification components (e.g. Identification code and password).	11.200 (a)(1)	N/A	F	X	X
UR.R064	**"Single Step" signature mode**	The first non-biometric electronic signature of a logon session shall be done by entering user id and password. In case of additional signatures needed during the same session, these signatures can be performed by inserting the sole password.	11.200 (a)(1) (i, ii)	N/A	F	X	X
UR.R065	**Electronic signature security**	The system should ensure that electronic signatures can be used only by the legitimate beneficiaries. Additional security procedures may be envisaged to achieve this assurance.	11.200 (a) (2), (b), (a) (3)	N/A	F	X	X
UR.R066	**Responsibilities change and delegating**	Procedures should ensure that the ability to apply electronic signatures is withdrawn for individuals whose responsibilities change, without the loss of information relating to signatures already executed. Procedures should cover the method of delegating signature responsibilities (e.g., periods of absence, holidays). (Data Integrity Guidelines)	N/A	N/A	P	X	X

3.1.4 Data Integrity Requirements

REQUIREMENT CODE	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	21 CFR PART 211; PART 11	EU GMP VOL4; ANNEX 11	P/F	APPL. (Y/N)	
						M/C CON	LES
UR.R067	**Data Integrity**	Data should be: A – Attributable L – Legible C – Contemporaneous O – Original A – Accurate	211.180 (a), (b), (c) 211.68 (b); 11.10 (b) 11.10 (c) 11.10 (e)	Vol.4 §4.1, §4.2, §4.10, §4.12 Annex 11 §4.8, § 7.1, §8.1, §9	P/F	X	X
		Attributable. It should be possible to identify the individual who performed the recorded task. The need to document who performed the task / function, is in part to demonstrate that the function was performed by trained and qualified personnel. This applies to changes made to records as well: corrections, deletions, changes, etc.		Vol.4 §4.20, c & f, §4.21, c & i, §4.29, e Annex 11 §2, §12.4, §15	P/F	X	X
		Legible. All records must be legible - the information must be readable in order for it to be of any use. This applies to all information that would be required to be considered Complete, including all Original records or entries. Where the 'dynamic' nature of electronic data (the ability to search, query, trend, etc) is important to the content and meaning of the record, the ability to interact with the data using a suitable application is important to the 'availability' of the record.		Vol.4 §4.1, §4.2, §4.7, §4.8, §4.9, §4.10 Annex 11 §7.1, §9, §10, §17	P/F	X	X
		Contemporaneous. The evidence of actions, events or decisions should be recorded as they take place. This documentation should serve as an accurate attestation of what was done, or what was decided and why, i.e. what influenced the decision at that time.		Vol.4 §4.8 Annex 11 §12.4, §14	P/F	X	X
		Original. The original record can be described as the first-capture of information, whether recorded on paper (static) or electronically (usually dynamic, depending on the complexity of the system). Information that is originally captured in a dynamic state should remain available in that state.		Vol.4 §4.9, §4.27, "Record" Annex 11§8.2, §9	P/F	X	X

REQUIREMENT CODE	REQUIREMENT NAME	REQUIREMENT DESCRIPTION	21 CFR PART 211; PART 11	EU GMP VOL4; ANNEX 11	P/F	APPL. (Y/N)	
						M/C CON	LES
		Accurate. Ensuring results and records are accurate is achieved through many elements of a robust Pharmaceutical Quality Management System. This can be comprised of: • equipment-related factors such as qualification, calibration, maintenance and computer validation. • policies and procedures to control actions and behaviours, including data review procedures to verify adherence to procedural requirements • deviation management including root cause analysis, impact assessments and CAPA • trained and qualified personnel who understand the importance of following established procedures and documenting their actions and decisions. Together, these elements aim to ensure the accuracy of information, including scientific data, that is used to make critical decisions about the quality of products.		Vol.4 §4.1, §6.17 Annex 11 "Principles", §5, §6, §10, §11	P/F	X	X

Note: the definitions above are based on the PIC/S PI-041-1 Data Integrity Guideline (July 1st 2021).

3.2 General Requirements

*The following paragraphs provide a set of user requirements divided into **categories** that have been identified by the Connected Machines Working Group as particularly related to connectivity of machines with supervisory systems.*

For each category this document provides a set of requirements that have been extracted from real documents coming from the pharmaceutical industry world-wide, classified into pre-defined categories, merged and if needed, ordered, improved eliminating specific product-related references.

Some categories such as cyber security and data analytics have been implemented with the input of all members of the working group and the result is the outcome of an effective team working to identify requirements from real experiences on the field.

Before the list of requirements, it is important to define the single requirement structure, taking into consideration the need for traceability of the requirements.

Each requirement should have:

1. *An unambiguous unique code.*
   The coding used for this section is:
   UR.F<CATEGORY#>.<REQ#>
   Examples of complete codes:
   UR.F001.01 – single requirement of category 1 (paragraph 3.2.12)
   UR.F012.01 – single requirement of category 12 (paragraph 3.2.12)
2. *A detailed description with possible related tables or pictures.*
3. *An indication of the obligatory level of the requirement (Must or Desirable).*
   All GxP requirements should be MUST.
4. *An indication of the criticality level of the requirement (type and impact size)*
   On Table 1 we supply the description of scenarios for the classes and for the levels used in order to assign such values to each requirement.

Moreover, a requirement can be structured in a hierarchy of sub-requirements (children) in order to detail some aspects of the general one (parent). In this case, in order to guarantee the traceability from the father, a child requirement will have a code derived from the parent's one obtained by adding a progressive number to its code.

Keep in mind that, in order to guarantee the traceability of requirements, it is necessary that each requirement is classified and classifiable. It must be avoided:

- *the union of several real requirements in a single requirement in the document*
- *the use of point/number lists for details of a single requirement.*

- *the duplication of requirements: the same requirement in various points of the document and even with different descriptions.*

In case of new revisions of the document, in order to maintain the traceability and to make easy the impact analysis of the new version on the project, it is important to highlight all changes with a visual indication regarding the status of the requirement.

Following rules should be applied:

1. *It must be avoided the re-use of removed codes. It should be given the evidence of the fact that a particular code has been removed (indicating it with the appropriate style: crossed)*
2. *It should be given the evidence of the fact that a requirement had been modified or added (during the last revision), indicating it with the appropriate style (Modified → Bold Style, New → Underlined) .*
   Moreover, on the Document Change History there should be a detailed list requirements that had been added, removed and modified.

The following sections include detailed requirements that will be subject to testing.

Each operational requirement is identified with the following information:

- Code: unique code of the UR (traceable to more detailed specification and verification step where applicable)
- Requirement description: brief description identifying the requirement to be satisfied
- Mandatory level
  - M: Must
  - D: Desirable

- Criticality class
  This information should be used by User to define the validation approach in the Validation Plan.
  - GxP: relevant to product quality
  - Safety: relevant to operator safety
  - Business: relevant to business risk

- Criticality level
  This data is fully applicable for GxP and Safety criticality classes. For business class requirements the level indication can be marked as N/A.
  Refer to Table 1 for details.
  - H: high impact
  - M: medium impact
  - L: low impact

Specific tables can be used as a reference by any requirements.

Tables for Mandatory, Criticality Class and Criticality Level are left empty as values should be assessed according to the specific application or Company policy.

Table 1 – Criticality scenarios

Following table provides the description of the different criticality scenarios for each criticality class.

For each class and for each level (High, Medium, Low) an applicable scenario must be defined.

The content of this table must be considered as an example. It must be verified and adapted to the specific application.

GxP Criticality Class *Specify scenarios using as methodology reference GAMP5 Appendix M3 paragraph 5.3.2.*	
Level	Scenario
H	*Major or irreversible side-effects on the patient (e.g. defects seriously impacting the efficacy, purity of the product), and/or critical defects on the product aspect.*
M	*Modest and reversible side-effects on the patient (e.g. defects impacting the efficacy, purity of the product), and/or significant defects on the product aspect.*
L	*Minor or negligible side-effects on the patient and/or aesthetical defects on the product aspect.*
Safety Criticality Class *Specify scenarios using as reference, for example, risks listed on Machinery Directive 2006/42/CE (Annex I, Point 1).*	
Level	Scenario
H	*Major irreversible injury or death*
M	*Reversible harm or injury on the operator*
L	*Minor or negligible effects on the operator*
Business Criticality Class *Specify scenarios accordingly. In order to define the "Risk to manufacturing (process) equipment" scenario it is possible to use the OEE (Overall Equipment Effectiveness) model to evaluate efficiency loss thresholds related to unfavourable events (H, M or L).*	
Level	Scenario
H	*Production break with loss of the production batch in progress and/or high time/costs for intervention (Machine stopped).*
M	*Production break without loss of the batch in progress (possible need of rework) and/or medium time/costs for intervention (Machine stopped).*
L	*Temporary production break with negligible time/costs for intervention.*

3.2.1 Recipes and Configuration Management

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.F001.01	The system shall be capable of setting and saving the process and operational parameters in a singular and identifiable recipe.			
UR.F001.02	The System shall be capable of managing recipes, meaning: - creating a new recipe, - editing an existing recipe, - printing/exporting/deleting a recipe.			
UR.F001.03	Adding or modifying a recipe shall not require changes to configuration or programming.			
UR.F001.04	Changes (including creation and deletion) to recipes shall be reported in audit trail.			
UR.F001.05	The recipe should contain the following data: - Recipe ID - Product Name / Number - Recipes operational values - Recipe version number *Fields listed here above might change according to machine type.*			
UR.F001.06	The System shall be capable of managing the recipe life-cycle. As a minimum, the System shall manage recipe versioning and recipe status.			
UR.F001.07	The System should manage recipe approval status (e.g. “Edit”, “Released”, “Retired”, etc.) to have a completely controlled life-cycle.			
UR.F001.08	The system should manage recipe status according to approval by supervisor or responsible			
UR.F001.09	Only approved, validated recipes should be accessible for runs on the control system for commercial production.			

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.F001.10	Retired recipes should not be displayed to the operators. Anyway, it shall be possible to retrieve all the recipes (even if already retired) if associated with a production order.			
UR.F001.11	It shall be possible to make online changes to development recipes during a production run under audit trail			

3.2.2 Audit Trail management

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.F002.01	The audit trail cannot be modified or deleted and the relevant function cannot be deactivated.			
UR.F002.02	The system must have the ability to automatically date and timestamp data that is stored electronically.			
UR.F002.03	Manual date/time change should not be possible.			
UR.F002.04	All events must be recorded in chronological order and can be displayed at any time for further analysis			
UR.F002.05	The audit trail must be able to be displayed on the screens by plain text message.			
UR.F002.06	The clear text messages must be printable/exportable (e.g. .txt / pdf / xml).			

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.F002.07	All records are unalterable, read-only and include: - User name - Timestamp (date, time) - Specify the occurred event (e.g. alarms), incl. acknowledgment - Old value, new value *Unalterability can be ensured by check-sum or other measures.*			
UR.F002.08	For critical events, the reason for the change should be included in the audit trail selecting from a pre-defined set of reasons.			
UR.F002.09	All users' actions/measures as well as the user, the acknowledgment of messages/alarms and the acknowledging user and the associated timestamp have to be recorded.			
UR.F002.10	All audit trail data shall be stored on the system itself or on Corporate device available for audit trail review with a specific period or frequency to be defined.			
UR.F002.11	Audit Trail should be generated by the system that manages the electronic record being changed. For example Audit Trail cannot be generated at LES level for actions done on process parameters managed by a specific equipment.			

3.2.3 Batch/Lot operations

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.F003.01	There must be a watch dog to monitor the communication between each single machine and Line SCADA/HMI system			

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.F003.02	The vendor shall implement OPC UA as the preferred communication protocol for the data transfer to / from the system.			
UR.F003.03	The control system must be able to exchange information with the upper level system (LES and/or MES). Examples: alarms, statuses, set-points, alarm limits, commands, audit trail			
UR.F003.04	The control system must be able to function independently, without LES (remote/manual mode), which can be selected by the operator on local HMI.			
UR.F003.05	Customer IT Services (e.g.: LES, MES, ERP, etc.) shall be able to exchange data with each Individual machine such as variable data for vision systems (e.g. batch no., expiry date, production date etc…)			
UR.F003.06	The run-enable of all equipment shall be performed through the LES			

3.2.4 Data Integrity

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.F004.01	The system must have the ability to prevent deletion of electronic records if not already transferred on other official repository			
UR.F004.02	The system must prevent overwrite Audit Trail data / files.			
UR.F004.03	The system may link an electronic signature to the corresponding electronic record to prevent data manipulation			
UR.F004.04	The system must have the ability to automatically date and timestamp data that is stored electronically			
UR.F004.05	Date/Time stamp is based on a system clock which is set correctly and continually via			

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
	automatic synchronization from a certifiable source.			
UR.F004.06	It must be ensured that the changeover between summer and winter times operates correctly in computers and control systems. In this context there should be no problems with data analysis.			
UR.F004.07	Date/Time format should be clearly documented (e.g.: time-zone identification).			
UR.F004.08	Raw data must be retained and protected as originally generated. The data collected must be recorded at the same time as the action is performed. It must be correct, complete, accurate and attributable (to a person or source).			
UR.F004.09	A backup & recovery procedure must be available for the entire system. The procedure must be documented in the operating instructions and tested as part of the qualification.			
UR.F004.10	A backup and restore method is provided by the supplier ensuring that any part of the system, including application(s), electronic records, metadata, audit trails, recipes, alarm history, electronic signature, system settings and configuration, can be restored in the event of a system emergency or disaster.			
UR.F004.11	An automatically migration of all GMP-relevant project data must be possible in case of software updates. The data may not be changed.			

3.2.5 Operational Efficiency

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.F005.01	The control system should provide statistical processing capability to report various OEE statistics.			
UR.F005.02	Machine OEE shall be calculated as Production Availability * Production Performance * Production Quality (in percentage format)			
UR.F005.03	Production and reject data shall be listed to include quantity produced and rejects by type.			
UR.F005.04	It should be possible to generate following reports: - Waterfall report - OEE analysis - Production by entity - utilisation analysis - utilisation timeline			
UR.F005.05	OEE shall be displayed per PO, per shift, per day, per working week.			
UR.F005.06	Any machine downtime caused by fault on machine i.e. sensor failure, overload, etc. shall be captured automatically from signals from the PLC."			

3.2.6 Critical GxP parameters and process data monitoring

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.F006.01	Alarms that are related to process Critical To Quality (CTQ) parameters should be distinguished versus non-critical alarms on the user interface and on the EBR			
UR.F006.02	The response time from the signal and data acquisition must be object to a specific			

	assessment in order to take in account the time constant of the process.			
UR.F006.03	The equipment MUST expose all Critical Process Parameters via OPC-UA for data collection by external systems			

3.2.7 Data Analytics

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.F007.01	The system must make available a list of data for external use, these data must be fully documented and must be collected through standard interfaces (i.e. OPC UA, API REST, SQL ODBC). *Please select your preferred interface*			

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.F007.02	Data should be classified according to "acquisition frequency" 1) Sensors/Actuators data (high frequency) (i.e. safety sensors, accelerometers, etc.) 2) Functional unit data (medium frequency) (i.e. quality control data, vision inspection, etc.) 3) Machine data (medium/low frequency) (i.e. alarms, information alerts) 4) Line data (low frequency) (i.e. performance data, settings/status/diagnostic data) High frequency data are typically aggregated and exchanged together with Medium/Low frequency data for Data Analytics purposes. *High/Medium/Low frequency depend on the process. Example of frequency ranges for a process machine:* *- High: 1 µsec – 100 msecs* *- Medium: 100 msecs – 1 sec* *- Low: 1 sec - 1 min*			
UR.F007.03	Data should be classified by "scope" 1) Machine control data 2) Machine diagnostic data 3) Process control data 4) Process diagnostic data 5) Cyber security monitoring			
UR.F007.04	Performance reporting - a collection of reports should be available to help monitoring the efficiency of production process (i.e. OEE)			
UR.F007.05	Diagnostic reporting - a collection of reports should be available to monitor the health state of the Machine/Line and informing about suggested maintenance actions			

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.F007.06	Edge analysis - Should be possible to access some reports directly on Machine/Line level, this reduces the required communications bandwidth between machines and plant by performing analytics and knowledge generation at or near the source. It allows near real-time decisions from data at the right level even without top network access.			
UR.F007.07	Mobile analysis - Should be possible to access some reports from mobile devices (Tablets/Smartphones), this allow to be informed remotely (i.e smart working) when not real time decisions are required			

3.2.8 Exception Handling

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.F008.01	In order to ensure that safety and quality critical parameters are properly monitored, an alarm strategy shall be established to differentiate between alert levels and action levels.			
UR.F008.02	The Vendor will provide a list of all possible alarms/alerts (audible and visible) applicable to the specified machine(s) classified to critical (which could influence machine operation safety and/or correctness) and non-critical (which could be considered as notifications). For each alarm, triggering sensors or conditions shall be specified.			

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.F008.03	Design criteria to consider when designing an alarm management application are: - Alarm levels definitions (product critical, operational safety critical, warning, alert) - Alarm notification (visual, audible) - Alarm colour scheme - Alarm acknowledgement strategy (single vs. multiple acknowledgement) - Alarm state definition (active/unacknowledged, active/acknowledged, inactive/ unacknowledged, inactive/acknowledged) - Alarm commenting capabilities - Assignment of alarms to operating areas (alarm filtering) - Alarm data exposure to supervisory system			
UR.F008.04	An alarm summary page shall be provided at each operator interface including connected supervisory system			
UR.F008.05	Alarm / error messages are to be displayed and transferred to connected supervisory systems as codes and also plain text (no shortcuts or just codes) to ensure proper interpretation by end-user. Alarms shall be presented to the user in a way that allows to have clear situation awareness and with the following priority (as an example): 1. Safety related alarms 2. Technical alarms 3. GMP/Quality alarms 4. Notifications			
UR.F008.06	Alarm log shall permanently store all alarms and events locally or on a centralised system connected on the network.			

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.F008.07	Batch report for GMP alarms shall include the following information, as a minimum: o Alarm identifier o Alarm category o Alarm description (that clearly describes the alarm) o Alarm status o Time and date activated o Time and date acknowledged, and by whom (User I.D) o Time and date alarm cleared o Batch Number / Lot Number			
UR.F008.08	The control system shall be capable of automatically re-establishing communications following an internal or external communications fault without manual intervention.			

3.2.9 Electronic Batch Record

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.F009.01	An electronic batch record system is a replacement for paper batch record system and shall be capable of providing the following: - The ability to perform batch release by exception (focus on OOSs) - An unalterable batch record - The ability to collect data from all levels of a computer system - A full audit trail of the production data collected			
UR.F009.02	All reports related to the batch, in a not changeable and human readable format, shall be exported, transferred onto a network share or printed to a network printer.			

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.F009.03	The system shall be capable of providing a run report with detailed information on production or WiP/CiP batch execution.			
UR.F009.04	Information to be displayed might include the following information: • Production information (name of the product, batch number, counter for all products (good, rejected)…) • System parameters (set and measured values) • Batch statistics • Production statistics (OEE) • Alarms (critical, non-critical) and alarm limits • Help screens (Fault assistance)			
UR.F009.05	The data should be collected and processed, aggregated in graphic forms, available for further analysis (quantitative and qualitative).			
UR.F009.06	It also should be possible to filter/configure the selection of data for the Batch report			
UR.F009.07	The System shall be capable of interfacing with External Historical Systems to record GMP and non GMP data.			
UR.F009.08	In case serialization is required in the production line, the system should provide all data required to satisfy the relevant requirements.			
UR.F009.09	In case Material Tracking is required in the production line, the system should provide all data required to satisfy the relevant requirements.			

3.2.10 User Management and Access Control

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.F010.01	The system must be protected against unauthorized access through a person-specific identification.			

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.F010.02	User authentication shall be done using a unified user management system across different machines such as active directory.			
UR.F010.03	The application should have different user groups such as: - Process operators - Line leaders - Maintenance engineers - Automation engineers / System - Administrators In case of centralised user management, user groups should be consistent with network Domain User Groups.			
UR.F010.04	The functions to which each user can access must be reported in a list. The list must be kept up to date and can be generated by the SW or included in the documentation.			
UR.F010.05	Each HMI shall display the current user that is logged onto the system and let the Supervisory System (e.g.: LES) to know remotely which is the current user on each machine.			
UR.F010.06	Access to all data and metadata, including audit trails, must be restricted to enable correct operation of the application and prevent “back door” access (by effectively bypassing the application-based security).			
UR.F010.07	Login and Logoff actions on the system must be recorded; the record must include rejected login attempts.			
UR.F010.08	If connection to domain fails, local user/groups will be available as emergency users.			
UR.F010.09	No access to the operative system should be possible by any not authorized users (e.g.: only administrators or automation engineers can access it).			
UR.F010.10	Password Display: The system shall not display the authentication password in clear text on the screen when entered.			

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.F010.11	Automatic Log out: After a configurable period of inactivity, set by the system administrator, the system must automatically log out the current user.			
UR.F010.12	The system must be capable of automatically forcing users to change passwords on a scheduled basis once the administrator configures the duration before change time limit. The system should prevent reuse of the password.			
UR.F010.13	A list of active users should be available.			
UR.F010.14	Security for data and operator access shall be provided using a user ID/password, or some other agreed method. The password must meet User's password requirements for minimum password length, complexity and expiration policy			

3.2.11 Cyber Security

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.F011.01	In the design of the system and definition of its network architecture, Cyber Security aspects shall be considered. For illustrative, not limiting, purpose: malware protection, CVE mitigation, etc. considering IEC 62443 as standard reference.			
UR.F011.02	In case of remote access for machine maintenance reasons, it is to be considered IEC 62443 as standard reference.			

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.F011.03	Minimise interface points (between machine and external network) and properly segregate networks (e.g.: internal real-time network vs. external network) (refer to IEC 62443).			
UR.F011.04	Network exposed Automation Control Components (e.g.: PLC, iPC, etc.) and relevant Operating System & Software packages should be up-to-date (e.g.: recent proven and supported versions having a long-life ahead).			
UR.F011.05	Computerised system should allow execution of centralised Cyber Security tools and services such as: - ZeroDays notification - Anomaly Detection - Penetration Test - Syslog with SIEM – Security Information Event Management). Usage of specific solutions/tools to ensure Cyber Security should be defined with a risk-based approach.			
UR.F011.06	In case of remote access, Computerised system should notify, log the access to the end-user and be compatible with existing access security policies.			
UR.F011.07	The remote assistance could be possible using an engineering workstation (physical or virtual) provided by customer and segregated by the system by a custom managed firewall (ensuring IP).			
UR.F011.08	All data sent outside the customer plant (i.e. Cloud) has to be encrypted.			
UR.F011.09	Should be always possible for the customer to access to the data transfer configuration without vendor support (Confidentiality Check).			

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level

3.2.12 Remote control

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.F012.01	A Remote Connectivity feature must be installed on the system, to provide the remote help and tele-diagnosis.			
UR.F012.02	The feature should be activated with explicit action by end user in order to reduce risk of intrusion by unauthorised personnel.			
UR.F012.03	Direct exposure of the equipment on internet is never considered acceptable, a proper VPN system shall be designed and implemented to guarantee connection protection and traceability			
UR.F012.04	The feature should be automatically deactivated after a configurable time out in order to avoid the risk of user deactivation forgetfulness			

4 DETAILED REQUIREMENTS FOR UNIT DOSE VIALS (UDV) MONODOSE STERILE PACKAGING LINE

This chapter contains the detailed requirements for the UDV packaging line, limited only to connection and data exchange.

The chapter should serve as a specific application example of the general principles described in the previous chapters.

The specific data and messages to be handled (in / out) and transferred to the LES are specified including source and destination.

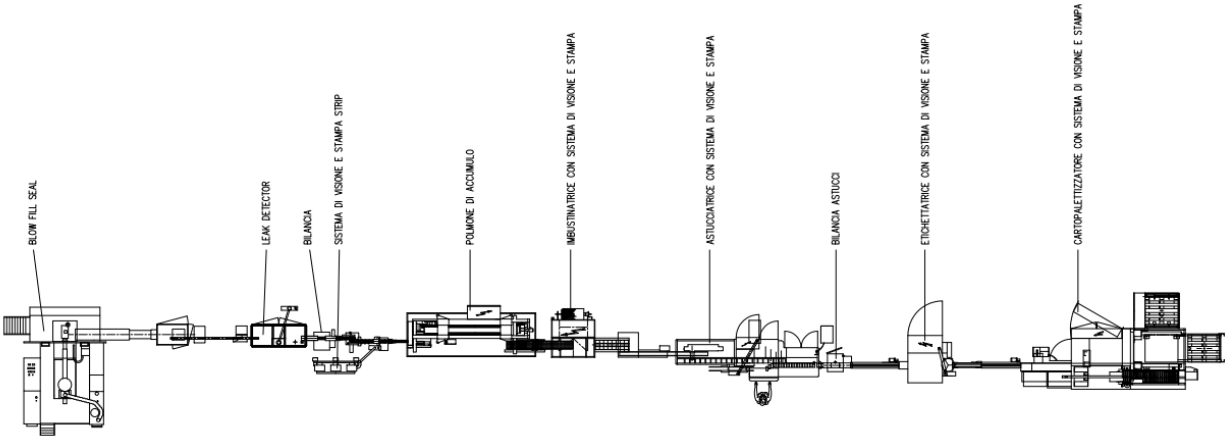
4.1 System / Project Overview

As a case study it has been selected a packaging line of single dose sterile: UDV (Unit Dose Vials). It is a real case line existing by the Chiesi Farmaceutici manufacturing site in Parma.

The line consists of the following machines and devices:

Typology	Local HMI	Note
Blow Fill Seal	Yes	
Leak detector	Yes	
Check weigher	Yes	
Strip printing and vision system	Yes	Printing of variable data on the vial
Storage buffer	Yes	
Overwrapping machine with printing and vision system	Yes	
Cartoning machine with printing and vision system	Yes	
Box check weigher	Yes	
Labeller (label printing and vision system)	Yes	Printing of variable data on the blister
Cartopalleting machine with printing and vision system	Yes	

The line is connected to 2 holding tanks, installed in the upstream preparation department, that feed the line with the product to be packaged.



Line layout

4.2 Applicable Standards

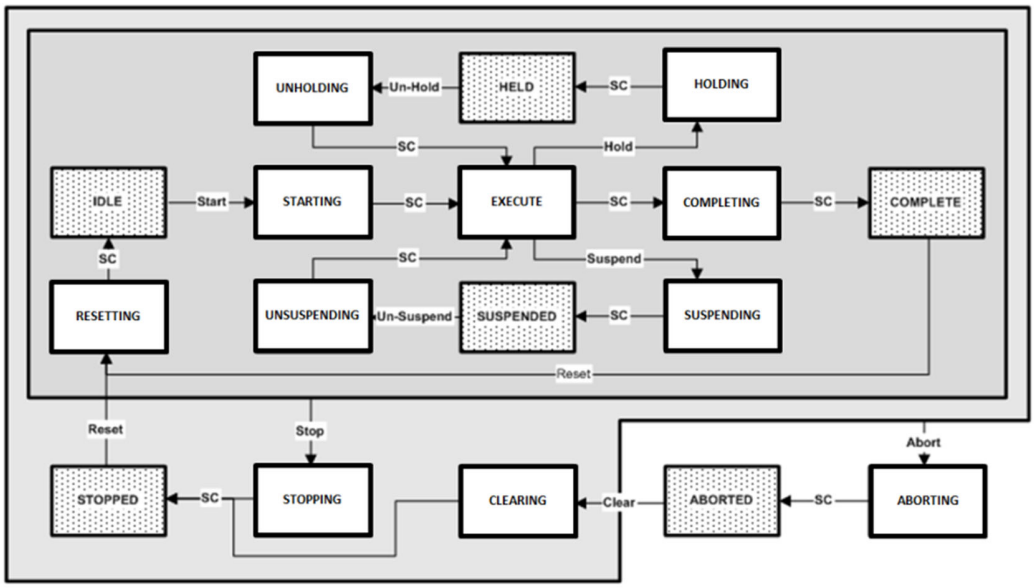
In this section are given general information on the standards that we assumed to apply.

4.2.1 PACKML – ISA TR 88.00.02

The PackML standard defines a reference model of a generic packaging machine in order to map the exchange of information necessary to interact with this machine.

4.2.1.1 PackML Reference Model

Machines should implement a state model as defined in PackML standard.
At least the minimum required as described in following tables.



SC = State Complete

IDLE = Wait State

EXECUTE = Acting State

With the following states:

ANSI/ISA-88.00.01 Procedural States	ISA-TR88.00.02 Equipment States				
	Value	Unit / Machine States	Wait	Acting	Minimum Required
<not defined>	1	Clearing		x	
Stopped	2	Stopped	x		x
<not defined>	3	Starting		x	
Idle	4	Idle	x		x
Paused	5	Suspended	x		
Running	6	Execute	x	x	x
Stopping	7	Stopping		x	
Aborting	8	Aborting		x	
Aborted	9	Aborted	x		x
Holding	10	Holding		x	
Held	11	Held	x		
Restarting	12	Unholding		x	
Pausing	13	Suspending		x	
<not defined>	14	Unsuspending		x	
<not defined>	15	Resetting		x	
<not defined>	16	Completing		x	
Complete	17	Complete	x		

And the following operating modes:

ANSI/ISA-88.00.01 Example Modes	ISA-TR88.00.02 Control Modes	
	Value	Unit / Machine Control Modes
<not defined>	0	Invalid
<not defined>	1	Production
<not defined>	2	Maintenance
<not defined>	3	Manual
<not defined>	04 – 31	User Definable

4.2.1.2 Pack Tags Reference

According to the modes, the relevant states and the commands to change the states, PackML defines the structure of the data (under the form of Tags) that allow the interface with the machine so that it can be controlled as an element of an overall production line.
Machines should implement at least the minimum required status and command TAGS as defined in PackML standard and described in following tables:

PackTags: Minimum required for information/machine monitoring

STATUS TAGS						TAGNAME	DATATYPE
UnitName						UnitName	PackMLv30
	Status					UnitName.Status	PMLs
		UnitModeCurrent				UnitName.Status.UnitModeCurrent	Int (32bit)
		StateCurrent				UnitName.Status.StateCurrent	Int (32bit)
		MachSpeed				UnitName.Status.MachSpeed	Real
		CurMachSpeed				UnitName.Status.CurMachSpeed	Real
		EquipmentInterlock				UnitName.Status.EquipmentInterlock	Bool Structure [2]
			Blocked			UnitName.Status.EquipmentInterlock.Blocked	Bool
			Starved			UnitName.Status.EquipmentInterlock.Starved	Bool
ADMIN TAGS						TAGNAME	DATATYPE
UnitName						UnitName	PackMLv30
	Admin					UnitName.Admin	PMLa
		ProdProcessedCount[#]	Count			UnitName.Admin.ProdProcessedCount[#].Count	Int(32bit)
		ProdDefectiveCount[#]	Count			UnitName.Admin.ProdDefectiveCount[#].Count	Int(32bit)
		StopReason	ID			UnitName.Admin.StopReason.ID	Int (32bit)

PackTags: Minimum required for supervisory control

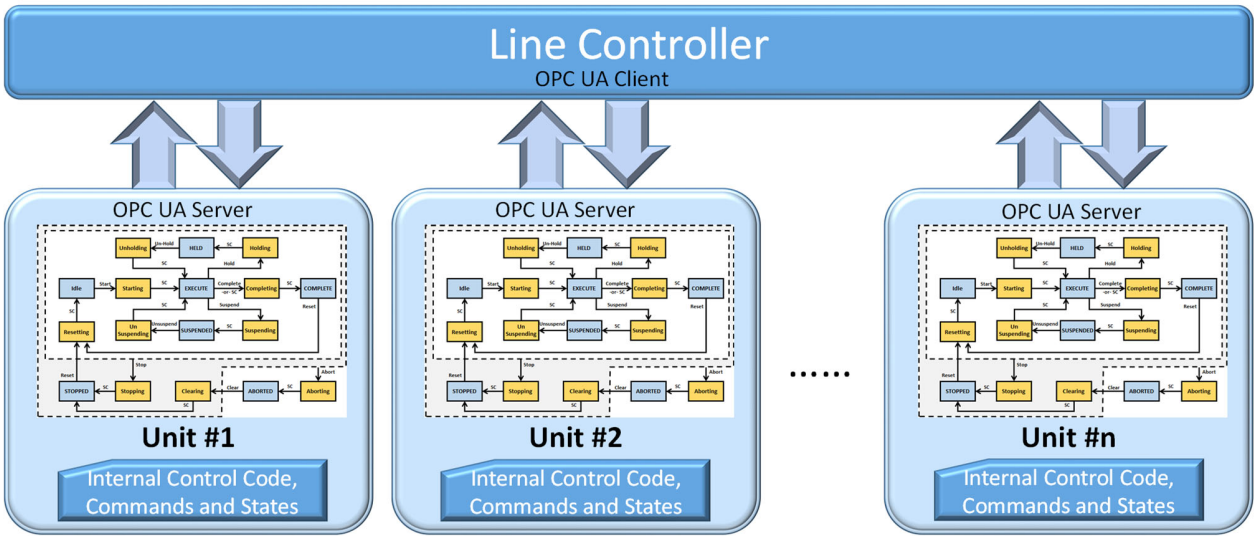
COMMAND TAGS						TAGNAME	DATATYPE
UnitName						UnitName	PackMLv30
	Command					UnitName.Command	PMLc
		UnitMode				UnitName.Command.UnitMode	Int (32bit)
		UnitModeChangeRequest				UnitName.Command.UnitModeChangeRequest	Bool
		MachSpeed				UnitName.Command.MachSpeed	Real
		CntrlCmd				UnitName.Command.CntrlCmd	Int (32bit)
		CmdChangeRequest				UnitName.Command.CmdChangeRequest	Bool

4.2.1.3 Quality & Production Data Sharing

For the reporting of production and quality data – See the Table ADMIN TAGS:
Administration tags are used to describe the quality and alarm information of the unit machine. Administration tags include alarm parameters which describe the conditions within the base state model typically for production data acquisition (PDA) systems. The administration tags also include parameters which can describe how well the machine operates, or specific information on the product quality produced by the machine. Administration tags generally originate from the unit machine and can be used on the HMI or a remote system.
Some administration tags support transfer of data for OEE calculations. Refer to ISO 22400 for information concerning measurement of key performance indicators (KPIs), including OEE.

4.2.2 OPC-UA

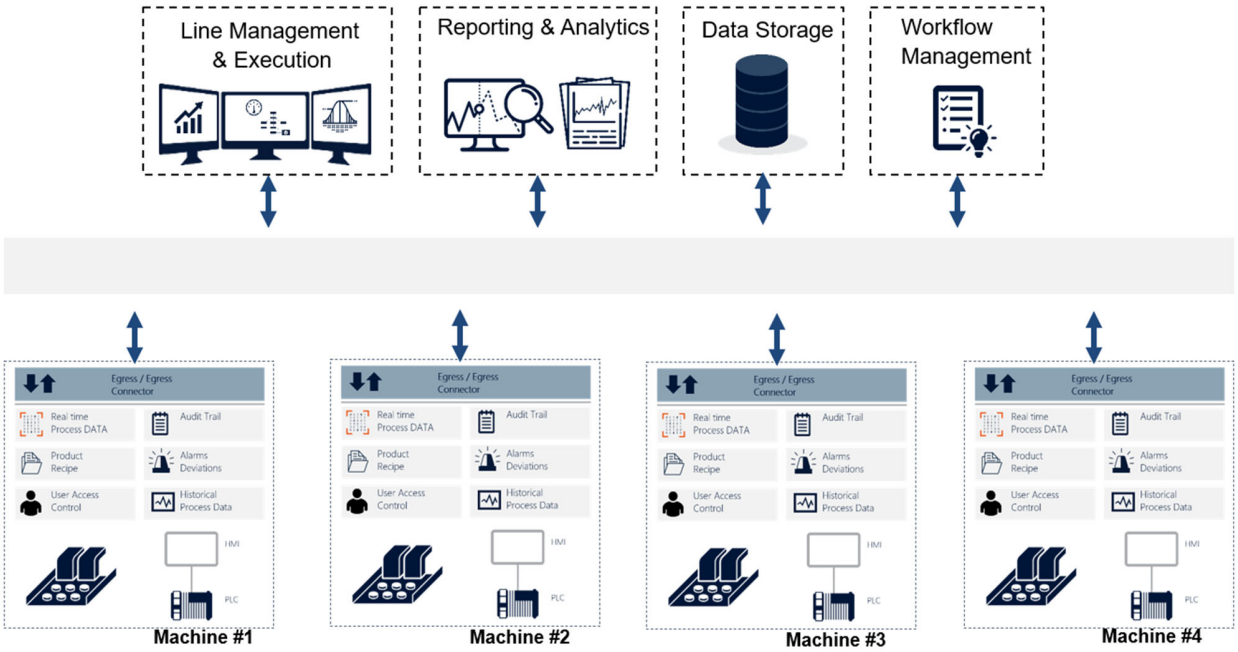
The figure illustrates the scope of PackML in a typical environment, with units acting as OPC UA Servers and a (generic) Line Execution System as an OPC UA Client application. It defines a standard set of interfaces to and from a unit/machine, so that it can be controlled as an element of an overall production line. It maps the internal states of the unit into a standard state model, and internal commands into a standard set of commands, hiding the details of the actual implementation of the unit's code.



Source: OPC UA for PackML 1.0.0 Companion Specification V09

4.3 Functionalities of a Line Execution System

In this paragraph we define the functions of a generic Line Execution System, or a system in charge of coordinating activities. In order to focus on these coordination functions required for the correct functioning of the line, the allocation of these functions to a specific system has been intentionally omitted, i.e. omitting to identify which system should perform these functions. In particular, it was assumed that there is no MES system available in the company (indeed this is the most common scenario in the case of medium-small companies). It is only assumed that an ERP is available, which is in charge to assign a Batch ID.



This representation summarizes the functions expected at the machine level and at the Line Management level.

In the following, are defined the information flows between the machine and the generic LES.

4.3.1 Recipe management

The LES shall align to the recipes/formats available in the machine. In this way the LES shall allow to associate each recipe/format to the relevant product code. At this purpose, the following functionalities shall be available:

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.L001.01	Upon LES request, the machine shall upload the list of recipes/format currently available and managed on the machine itself with the following information: • Recipe ID • Version (if available) • Product code (as applicable) • Description • List of parameters			
UR.L001.02	The LES shall allow the association of each product with the corresponding recipes/format available on the machine (as applicable) with the addition of the (variable) parameters (as applicable).			

4.3.2 Opening the Batch

At the opening of a new batch the LES manages the following information:

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.L002.01	The LES shall allow the registration of the change of format, as applicable, even if it is only a mechanical setup.			

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.L002.02	The LES shall allow to start the "QC Run" function: challenge of the reject mechanisms of non-conforming products, and its registration. The single machine of the line shall be able to run without any batch loaded to allow maintenance technicians to perform setup or change-over.			
UR.L002.03	The LES shall allow the manual entry by the operator of the batch data: • Work Order and/or Batch ID from ERP (whether or not bar code or QRcode) • Product code • Description • Qty to be produced • Production and expiry date • Information leaflet / case			

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.L002.04	The operator / LES identifies the recipe to be activated for each machine (including any IPC system). The recipe can be associated to the Product code or selected by means of a cross reference table derived from the machine list of recipe of req UR.L001. In addition (or as an alternative) the following data shall be input for each machine (as applicable): • Variable Data: A set of format parameters linked to the product that LES sends to the machine (for example, expiry date in the appropriate format on the stamping machine and cartopallet). • Critical process parameters could also be included (i.e. the number of packages per unit that are used to allocate the number of codes for serialization) but for now we assume that they are resident in the machine.			
UR.L002.05	• The LES shall allow the Double check: confirmation of correct data entry by a second operator.			

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.L002.06	Once the above information have been provided the LES can coordinate each machine of the line: • "Sending" the recipes to the various machines. Refer to the info to be entered for setup of each machine in the tables of the following paragraph. • Verification of the correct reception of data from the machines • Enabling the start of production. Ideally the operator doesn't have to go machine by machine to start each one.			

4.3.3 During batch execution

During the Batch execution, the following functionalities are expected from the LES:

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.L003.01	Provide information regarding the process in progress (Dashboards, including OEE, dynamic synoptics, ...)			
UR.L003.02	Acquisition and storage of (at least) GMP critical parameters at line level (assuming that a centralized historian is not available). These data must be associated with the batch ID.			

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.L003.03	Acquisition and storage of significant GMP events including line and / or machine Audit Trail. The acquisition of the Audit Trail must in any case take place even before the start of the batch. The audit trail shall be generated both when a batch is active and during the machine downtimes, eventually batch number shall be included when a batch is running.			
UR.L003.04	Acquisition and storage of all machine alarms (with alarm classification, e.g. GMP critical).			
UR.L003.05	LES System should manage In Process Controls (IPC).			
UR.L003.06	Capability to send a notification to the line supervisor and to the QA team in case of GMP deviation (following a truly critical alarm that requires the opening of an investigation, e.g. particle count out of range on an aseptic filling line). The notification shall be triggered by the alarm, acknowledgment and return of the alarm. The event can be commented by the operator. In less critical cases, the action of a supervisor may be required.			
UR.L003.07	Change of (some parameters of) format in case of sublots of the same batch (if managed with the same batch record).			

4.3.4 Batch Closing

At Batch closing the LES shall collect / record the following activities:

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.L004.01	The LES shall allow to command the emptying of residual packages and its registration.			
UR.L004.02	The LES shall allow to command the emptying (removal of packaging, labels and other residual materials ...) and its registration.			
UR.L004.03	The LES shall allow to command the Reconciliation and its registration: • Count of materials delivered (in-feed), rejected (for each reject point) and check that no material is missing. • Reconciliation is used to prevent potential mix-ups. So it's required a consistency check of the physical counts of the materials. • The use of line meters may not be effective as reworking is allowed, therefore reworking that consists in putting rejected but reusable materials back online must be input to the system. • Automatic counters can be used for primary packaging reconciliation (and for investigations. Efficiency is managed through waste counts, but it is independent of reconciliation.			
UR.L004.04	The LES shall allow the registration of the Sticking of labels stating the "dirty" status of the machine, as applicable.			

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.L004.05	It should be possible to review batch data saved by the LES. For data in dynamic format, e.g. trends, list of alarms or Audit Trail (of configuration parameters) there should be functions supporting review (zoom, selection filters, ...) or at least the possibility of exporting the data in a format that can be consulted in electronic format.			
UR.L004.06	It shall be possible to generate a Batch Report, including: • Exception report (anomalous conditions automatically detected by the system (EU GMP Annex 11)) • Counters • Audit Trail • Trends ...			
UR.L004.07	It shall be possible to Review the data and related metadata for the Batch Release (Including Audit Trail [The Audit Trail section should ideally be stored in electronic format to facilitate consultation by the QA at the end of the batch])			
UR.L004.08	It shall be possible to Backup the data: • Manual backup to external USB hard drive • Automatic on centralized repository on the network Mechanism to prevent backup tampering (e.g. hashing) shall be in place.			

4.3.5 Long-term data management

The data must be kept for one year after the expiry of the product or according to company rules, ensuring that the integrity of the data is maintained.

It is necessary to ensure the ability to access this data for the entire retention period.

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.L005.01	For long term data it shall be possible to archive data with write access for administrators and read-only access for QA and production staff. For data in dynamic format, e.g. trends, list of alarms or Audit Trail (of configuration parameters) there should be functions supporting review (zoom, selection filters, ...) or at least the possibility of exporting the data in a format that can be consulted in electronic format.			
UR.L005.02	It shall be possible to export Data in a standard portable / searchable format also by third-party systems (eg. SQL).			

In case Data are stored in their native format (such as in case data retained by means of their backup copy) it is necessary to ensure the availability of the software that generated the data in order to be able to review them.

4.4 Unit Dose Vials (UDV) Packaging Line Parameters

In this section the process parameters for each machine of the UDV line are described.
For each parameter it is to be defined a corresponding PackML Command Tag.
The list of parameters do not pretend to be exhaustive: but each end user will have to check the parameters actually applicable for his/her own line.

4.4.1 Blow Fill Seal

It is assumed that recipes are stored locally: within the machine control system.

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.D001.01	**Control Modes** In addition to the PackML standard modes: 0 Invalid 1 Production 2 Maintenance 3 Manual The following custom modes are defined: 4 = CIP 5 = SIP 6 = Drying			
UR.D001.02	**Machine states** In addition to the PackML (minimum) standard modes: Stopped Idle (see below different types of Idle) Suspended (for external condition like blocked/starved event) Execute Aborting The following machine states are defined: Dirty (idle for Cleaning), Clean (idle for Sterilization), Sterilized (idle for drying) Dryied (idle for production)			

UR.D001.03	**Data to be input before the mode <u>production</u> starts**
	The machine requires the following parameters before starting a new batch:
	• Batch ID
	• Production Recipe ID
	• Product Parameters:
	  • Extruder speed
	  • Blow fill temperature
	  • Sealing pressure
	  • Filling time			

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.D001.04	**Data to be input before the mode cleaning (CIP) starts** The machine requires the following parameters before starting a new batch: • Batch ID • CIP Recipe ID • Washing Phase number (that interacts with the feeding tanks control system), associated to the Batch ID • 3 prewashing phases, 3 washing phases, 3 rinsing phases (actually only reading of variables and phases conclusion status) • Final Conducibility set point			
UR.D001.05	**Data to be input before the mode sterilization (SIP) starts** The machine requires the following parameters before starting a new SIP (usually after a CIP): • Sterilization Phase number (that interacts with the feeding tanks control system), *(SIP parameters are not product dependent)* • Sterilization time and temperature			
UR.D001.06	**Data to be input before the mode drying starts** The machine requires the following parameters before starting a new drying (usually after a CIP or SIP): • Batch ID (actually there is no dependency if the drying from the product) • Drying Phase number *(Drying parameters are not product dependent)*			

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.D001.07	**Data to be recorded during the mode <u>production</u>** The system will provide the following data to be recorded (in addition to the minimum "Admin Tags" in PackML): • Fill time (5 vials x 4 molds) • Temperature (about 11) • Filled vials nr. (filled vials, unfilled vials, discarded vials are counted downstream) • Extruder speed • Machine status (dirty, clean, sterile; the latter also expires after a configured period of time). It prevents the product loading. • Conductibility • Feeding buffer (product feeding pressure affects the vials filling) • Air pressure (it affects the sealing pressure and/or the buffer pressure) Critical parameters for batch release, in a Review By Exception scenario are product dependent, but in our case (at least): • extruder temperature • conductibility			
UR.D001.08	**Data to be recorded during the mode <u>CIP</u>** The system will provide the following data to be recorded : • CIP result (event - Character string associated to a boolean in the PLC)			
UR.D001.09	**Data to be recorded during the mode <u>SIP</u>** The system will provide the following data to be recorded : • SIP result (event - Character string associated to a boolean in the PLC)			

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.D001.10	**Data to be recorded during the mode <u>Drying</u>** The system will provide the following data to be recorded : • Drying result (event - Character string associated to a boolean in the PLC)			
UR.D001.11	**Alarms** The following alarms are required: Product input Temperature > 50°C Product input Temperature > 40°C for too long Product Manifold Temperature > 50°C Product Manifold Temperature > 40°C for too long Feeding Buffer Temperature > 50°C Feeding Buffer Temperature > 40°C for too long			
UR.D001.12	**OEE** The following variables for OEE calculations are required: nr. of filled vials nr. of unfilled vials working time suspended time …			
UR.D001.13	**Metadata** The following Metadata of Critical Process Parameters shall be recorded (as applicable): • Decimal points • Allowed ranges (min/max) • Time stamping (during production) • Audit trail (of SetPoints) • Electronic Signature (of SetPoints)			

4.4.2 Leak Detector

No local recipes with production parameters available. Even if the PackML standard include some minimum modes and states, the actual simplest machines do not cover all of these, but only the mode 1 Production and the states 4 Idle and 6 Execute.

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.D002.01	**Control Modes** PackML standard modes: 1 Production			
UR.D002.02	**Machine states** PackML standard states: 4 Idle (including the status completed) 6 Execute			
UR.D002.03	**Data to be input before the mode <u>production</u> starts** The machine requires the following parameters before starting a new batch: • Batch ID • Product Parameters: ○ Minimum tension discharge channel (Volt) ○ Maximum tension discharge channel (Volt) ○ Test tension (Volt)			
UR.D002.04	**Data to be recorded during the mode <u>production</u>** The system will provide the following data to be recorded (in addition to the minimum "Admin Tags" in PackML): • Number of good strips • Number of expelled strips • Measured tensions			
UR.D002.05	**Alarms** No GMP alarms			

4.4.3 Check weigher

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.D003.01	**Control Modes** PackML standard modes: 1 Production			
UR.D003.02	**Machine states** PackML standard states: 4 Idle (including the status completed) 6 Execute			

UR.D003.03	**Data to be input before the mode <u>production</u> starts**
	The machine requires the following parameters before starting a new batch:
	• Batch ID
	• Production Parameters:
	  ○ Reference weight (g)
	  ○ Format			

UR.D003.04	**Data to be recorded during the mode <u>production</u>** The system will provide the following data to be recorded (in addition to the minimum "Admin Tags" in PackML): • Number of good strips • Number of rejected strips • Tare (g) • Maximum weight (g) • Minimum weight (g)			
UR.D003.05	**Alarms** No GMP alarms			

4.4.4 Strip printing and vision system

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.D004.01	**Control Modes** PackML standard modes: 1 Production			

UR.D004.02	**Machine states** PackML standard states: 4 Idle (including the status completed) 6 Execute			
UR.D004.03	**Data to be input before the mode <u>production</u> starts** The machine requires the following parameters before starting a new batch: • Batch ID • Product ID and/or content quantity • Production Parameters: o Expiry Date			
UR.D004.04	**Data to be recorded during the mode <u>production</u>** The system will provide the following data to be recorded (in addition to the minimum "Admin Tags" in PackML): • Number of good strips • Number of rejected strips			
UR.D004.05	**Alarms** No GMP alarms			

4.4.5 Storage buffer

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.D005.01	**Control Modes** PackML standard modes: 1 Production			
UR.D005.02	**Machine states** PackML standard states: 4 Idle (including the status completed) 6 Execute			
UR.D005.03	**Data to be input before the mode <u>production</u> starts** The machine requires the following parameters before starting a new batch: • Batch ID			
UR.D005.04	**Data to be recorded during the mode <u>production</u>**			

	Not Applicable			
UR.D005.05	**Alarms** No GMP alarms			

4.4.6 Overwrapping machine with printing and vision system

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.D006.01	**Control Modes** PackML standard modes: 1 Production			
UR.D006.02	**Machine states** PackML standard states: 4 Idle (including the status completed) 6 Execute			

UR.D006.03	**Data to be input before the mode <u>production</u> starts**
	The machine requires the following parameters before starting a new batch:
	• Batch ID
	• Product ID
	• Overwrapping format ID
	• Product Parameters:
	  • Preparation date
	  • Expiry date
	  • Bag control code			

UR.D006.04	**Data to be recorded during the mode <u>production</u>** Critical Process Parameters to be reviewed for the batch release • Right and left sealing plate temperature • Sealing pressure • Machine speed Parameters for OEE calculation: • Nr. of formed and filled bags • Nr. of formed but not filled bags • Nr. of bags produced • Nr. of bags with text OK			

	• Nr. of bags picked from the pick/place • Nr. of bags in the downstream machine • Production hours (machine in run/execute) • Production minutes (machine in run/execute) • Production hours (machine stopped) • Production minutes (machine stopped)			
UR.D006.05	**Alarms** • Sealing plate temperature outside limits.			

4.4.7 Cartoning machine with printing and vision system

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.D007.01	**Control Modes** PackML standard modes: 1 Production			
UR.D007.02	**Machine states** PackML standard states: 4 Idle (including the status completed) 6 Execute			
UR.D007.03	**Data to be input before the mode <u>production</u> starts** The machine requires the following parameters before starting a new batch: • Batch ID • Product ID • Box format • (variable) Product Parameters: • Prospect and box control code			
UR.D007.04	**Data to be recorded during the mode <u>production</u>** Parameters for OEE calculation: • Nr. of input wrapped strips • Nr. of produced boxes • Nr. of discarded boxes			

	• Nr. of boxes picked from the pick/place			
UR.D007.05	**Alarms** No GMP alarms			

4.4.8 Boxes check weigher

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.D008.01	**Control Modes** PackML standard modes: 1 Production The following custom modes are defined: 7 = Calibration			
UR.D008.02	**Machine states** PackML standard states: 2 Stopped (actually Shut_down) 3 Starting (actually Warm_up), 4 Idle (actually Ready) 6 Execute (actually Run) 8 Aborting (actually Warning, Alarm, Setpoint ok, Out)			
UR.D008.03	**Data to be input before the <u>production</u> mode starts** The machine requires the following parameters before starting a new batch: • Batch ID (for the report) • Product name • Box format • Reference weight • Tare • Acquisition time • Acceptance thresholds (T1, T2, etc.)			
UR.D008.04	**Data to be recorded in the <u>production</u> mode** • Format version • Nr of boxes processed • Nr of boxes rejected for out-of-range weight • Nr of boxes rejected			

	• Nr of accepted boxes (by acceptance zone T1+, T1-, T2+, T2-) • std. deviation of processed boxes • std. deviation of accepted boxes • average of processed boxes • average of accepted boxes • last product in input • last product in output • last product weighed			
UR.D008.05	**Alarms** No GMP alarms			

4.4.9 Labeller (label printing and vision system)

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.D009.01	**Control Modes** PackML standard modes: 1 Production			
UR.D009.02	**Machine states** PackML standard states: 4 Idle (including the status completed) 6 Execute			
UR.D009.03	**Data to be input before the mode <u>production</u> starts** The machine requires the following parameters before starting a new batch: • Batch ID • Product ID • Labelling format • (variable) Product Parameters [Application identifiers of the vision system]:			

	• [1] Gtin • [17] Expiry Date • [10] Batch for Data Matrix • [1002] Patient Batch • [11] Manufacturing date • [37] Quantity • [93] Item Code Plus optional human readables: • [1001] Expiry Date (Patient) • [1003] GTIN • [1005] Expiry Date • [1009] Booklet/Prospect Code			
UR.D009.04	**Data to be recorded during the mode <u>production</u>** • Nr. of produced packages • Nr. of packages with printout OK			
UR.D009.05	**Alarms** No GMP alarms			

4.4.10 Cartopalleting machine with printing and vision system

Code	Requirement Description	Mandatory Level	Criticality Class	Criticality Level
UR.D010.01	**Control Modes** PackML standard modes: 1 Production			
UR.D010.02	**Machine states** PackML standard states: 4 Idle (including the status completed) 6 Execute			
UR.D010.03	**Data to be input before the mode <u>production</u> starts** The machine requires the following parameters before starting a new batch: • Batch ID • Product ID • Printing format • (variable) Parameters: • Serial number of the corner label			

UR.D010.04	**Data to be recorded during the mode <u>production</u>** • All aggregation codes to be associated to the corner label			
UR.D010.05	**Alarms** No GMP alarms			

5 OPERATIONAL REQUIREMENTS

GAMP 5 - Appendix D1 - Paragraph 3.3 – Operational Requirements

Operational requirements include:

- *functions*
- *data*
- *technical requirements*
- *interfaces*
- *environment*

Process descriptions or flowcharts may be included as appropriate.

Special consideration will be given to critical GxP requirements. These will be clearly defined, with references to the relevant regulation, where possible.

All requirements will be verifiable.

It will be noted that some requirements may be difficult to define and verify because they are subjective and therefore may be subject to different interpretation. The measurement or acceptance criteria for these requirements will be specifically defined as part of the approved requirement.

This section

6 CONSTRAINTS

GAMP 5 – Appendix D1 – Paragraph 3.3.4 - Constraints

The constraints on the specification and operation of the system will be identified. The following will be addressed as appropriate:

- *compatibility, taking into account:*
  - *any existing systems or hardware*
  - *any regulated company strategy or policy*
- *availability*
- *reliability requirements*
- *maximum allowable periods for maintenance or other downtime*
- *statutory obligations*
- *working methods*
- *user skill levels*
- *expansion capability*
- *likely enhancements*
- *expected lifetime*
- *long term support*

7 LIFE-CYCLE REQUIREMENTS

GAMP 5 – Appendix D1 – Paragraph 3.3.5 – Life Cycle Requirements

Any specific requirements that may impact the supplier's development life cycle and any subsequent verification activities will be identified. If this information is already provided elsewhere this will not be repeated.

The following will be addressed as appropriate:

- *development requirements, (e.g., minimum standards to be met by supplier's methodology)*
- *procedures for project management and quality assurance*
- *mandatory design methods*
- *special testing requirements*
- *test data*
- *load testing*
- *required simulations*
- *factory acceptance testing*
- *how deliverable items are to be identified*
- *in what form deliverables are to be supplied (e.g., format and media)*
- *documentation the supplier is expected to deliver (e.g., functional specification, testing specifications, design specifications, user and maintenance guides or manuals)*
- *data to be prepared or converted*
- *tools*
- *training courses*
- *archiving facilities*

support and maintenance required after acceptance

This section contains specific requirements that the Customer communicates to the Suppler and that potentially are or will be defined in a Validation Plan document.

This approach allows the user to produce the Validation Plan only for internal use. User therefore does not need to provide that document to the supplier as the really important requirements are included in the current section.
The Supplier Quality and Project Plan documents are the answer to the requirements of this section.

8 GLOSSARY

Definition of any terms that may be unfamiliar to readership of the document should be provide

Acronym	Definition
CFR	Code of Federal Regulations
CiP	Clean-in-Place
DS	Design Specification
ERP	Customer Management System
FAT	Factory Acceptance Test
FS	Functional Specifications
GAMP	Good Automated Manufacturing Practice
GMP	Good Manufacturing Practice
HMI	Human Machine Interface
IQ	Installation Qualification
MES	Manufacturing Execution System
LES	Line Execution System
NEC	National Electrical Code
NEMA	National Electrical Manufacturers Association
NFPA	National Fire Protection Agency
OOS	Out Of Specification
OQ	Operational Qualification
OSHA	Occupational Safety and Health Administration
PAT	Process Analytical Technology
PLC	Programmable Logic Controller
PQ	Performance Qualification
SAT	Site Acceptance Test
SCADA	Supervisory, Control and Data Acquisition
SOP	Standard Operating Procedure
TM	Traceability Matrix
UDV	Unit Dose Vials (UDV), Monodose Sterile
URS	User Requirements Specification
WiP/CiP	Wash-in-Place

9 ATTACHMENTS

Insert in the table references to documents attached to the current URS.