OMRON

WHITEPAPER

Validation of Autonomous Mobile Robots used in the Pharmaceutical Industry

A guide to the validation of Autonomous Mobile Robots (AMR) used in pharmaceutical industry using OMRON components

SCOPE

The pharmaceutical industry has many standards and guidelines that need to be followed; among these there is a requirement that computerized systems must be validated. This white paper gives an overview on how an automated system can be validated. A specific section with practical examples of AMR-based systems applications using OMRON products is included. It is expected that the reader already has a basic knowledge of pharmaceutical regulations.

CONTENTS

INDEX

1 Validation requirements

1.1 Pharmaceutical legislation (EU and US)

Manufacturing processes in the Life Sciences industries are highly regulated by the so called GMP (Good Manufacturing Practice). Equipment and systems used in these processes are also regulated by the same rules. cGMP means “current GMP” since the regulations change from time to time.

Regulations exist for other activities performed in these industries, such as the GLP (Good Laboratory Practice), GCP (Good Clinical Practice), GDP (Good Distribution Practice), GVP (Good Vigilance Practice), collectively known as ‘GxP’ (where ‘x’ is a placeholder).

Regulations vary across different industry sectors (e.g. pharmaceutical finished products / active principles, medical devices, biologic products, blood products, vaccines, etc.), each having its own set of regulation, variable country by country.

In this document for simplicity we cover only manufacturing processes in the pharmaceutical industry (finished products or medical devices) and the regulations applicable in the European Union and United States. Very similar considerations are applicable for other regulated industries, processes, and countries.

Among the many requirements, almost all regulations worldwide require the validation of processes and the qualification of supporting equipment.

This document deals with validation of computerized systems used in pharmaceutical processes. It refers to the entire equipment for completeness but is focused on the control system and is further specialized on robot systems as application examples.

The main objective of this document is to provide a guidance for final users and system integrators, to help them understanding their regulatory burden and achieve compliance with the applicable regulations. OMRON, as a producer of components for the pharma industry, can help customers with documents like this and can also provide specialized support services to help final users to achieve validated systems.

> 🕮 *A detailed coverage of the regulations can be found in the OMRON White Paper document “Validation of Robot Systems used in the Pharmaceutical Industry”, published in 2015 [32].*

New Regulations and Guidance documents

Since 2015 there were no significant changes in the regulation, however there are significant news in the Guidelines from the Authorities and industry trends. The major changes are:

- Finalization of the Data Integrity Guidelines from MHRA, FDA and PIC/S (2016-2021)
- Publishing of the GAMP 5 Second Edition Guide (2022)
- Publishing of the FDA Draft Guide “Computer Software Assurance” (CSA) in 2022.

The EU GMP Annex 11 is currently under revision, and a new edition is expected by mid-2026. A Concept Paper has been published about the revision process. Major changes regard data integrity, cloud computing, IT infrastructures, digital transformation, AI (artificial intelligence) and machine learning, alignment with the FDA Computer Software Assurance Guidance for Industry (CSA), validation of "Agile methods", audit trails, information security.

Other recent changes regard updates in some EU GMP Annexes, e.g. Annex 1 and ICH Q9R1 (Quality Risk Management, though the document included in EU GMP Part III has not been yet updated).

1.2 Data Integrity

1.2.1 Regulatory Guidelines

All major Regulatory Agencies have finalized their guidance documents on the Data Integrity topic. The following table summarizes the current status of the documents:

Author	Title	Date	Document Structure	Status
EMA	Questions and answers: Good Manufacturing Practice	August 2016	Q&A	Final
FDA	Data Integrity and Compliance with Drug CGMP - Questions and Answers - Guidance for Industry	December 2018	Q&A	Final
MHRA	'GXP' Data Integrity Guidance and Definitions	March 2018	DI expectations and glossary	Final
PIC/S	Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments PI 041-1	July 2021	General and complete guide, well structured	Final
WHO	Guidance On Good Data and Record Management Practices (WHO technical report series; no. 996, Annex 5)	May 2016	General guide with appendices ALCOA Expectations (paper and electronic)	Final

The most complete and comprehensive document is the PIC/S Guide PI 041-1. It covers extensively all data integrity regulatory requirements. Thorough reading of this document is a must for anyone who want to seriously understand and manage DI requirements in regulated environments.

The PIC/S PI 041 Guide covers many topics, such as:

- Pharmaceutical Quality Systems and Data Governance Systems
- Data Integrity Requirements for Paper Based systems (Paper Records)
- Data Integrity Requirements for Computerized Systems (Electronic Records), including validation.

One of the key principles is Risk Management, as an essential step in any data integrity management process. The Guide helps understanding the concepts of Data Criticality and Data Risks. Regulated companies are required to analyze their computerized systems during validation and determine data criticality and the necessary controls to ensure data integrity for critical data.

1.2.2 GAMP Guidelines regarding Data Integrity

In the last few years ISPE/GAMP published several guidance documents that harmonize the general principles and help putting them in practice:

- GAMP Guide: Records and Data Integrity (Apr 2017)
- GAMP Good Practice Guide: Records and Data Integrity - Key Principles (Nov 2018)
- GAMP Good Practice Guide: Records and Data Integrity - Manufacturing Records (May 2019)
- GAMP Good Practice Guide: Records and Data Integrity - Data Integrity by Design (Oct 2020)

Coverage of the contents of these GAMP guides is far beyond the scope of this document. However they can be very useful for a further understanding of the requirements and the practical application of the general principles.

1.3 GAMP® 5 Second Edition

The first edition of the GAMP 5 Guide was published in February 2008. The Second Edition has been published in July 2022 to reflect changes in computer technology. The new edition still maintains the same key principles, but now includes many changes and additions to cover computer validation in a more modern fashion.

The main body of the document describing the five key principles is nearly unchanged, therefore all the details included in the Vision Systems White Paper [32] are still valid. The document also includes a potential list of validation activities and documents.

Agility is a core ingredient of the Second Edition. Together with a better recognition of agile software development, GAMP 5 encourages an agile, critical thinking and risk-based approach to assurance of software.

The main changes and the relevance for robot systems are summarized below:

1.3.1 Non-linear software development models

The new guide recognizes the largely non-linear, agile, and more cyclical nature of modern software development: Iterative, incremental, and exploratory models are therefore emphasized over older, linear models like the waterfall and V-Model.

* Source: GAMP 5 Second Edition, © ISPE GAMP 2022.

This model is mostly applicable for the developers of software product and system integrators / OEMs but can also be applicable for the end users when the application software is managed in iterative / incremental manner. Agile development is often applicable to robotic systems.

Agility is considered an important element in both the specification and testing. A new Appendix has been added to clarify these new expectations.

Following the updated GAMP recommendations is now easier to validate computerized systems that are subject to frequent modifications.

1.3.2 Changes in the documentation requirements

Documentation produced during the life cycle may vary depending on the reference model (linear software approach vs. agile). There's a further shift to risk-based records of information, held in appropriate systems, that consider the modern software lifecycle.

Risk Management remains an essential element of the validation approach for any computerized system, including robots, and the risk management principles remain nearly unchanged from the first edition.

1.3.3 Critical thinking

Critical thinking is a major cornerstone of computerized system assurance in the GAMP 5 Second Edition, as well as in the FDA's new (draft) CSA guideline published in September 2022.

The GAMP 5 Second Edition encourages appropriate, efficient, and risk-based assurance dependent on the risk profile of the software being implemented. This new approach can be extremely useful in robotic systems validation. However, critical thinking needs knowledge from experts.

1.3.4 Update of development appendices

The areas of GAMP 5 focusing on requirements specifications (RS) have been adjusted to reflect the new world of modern, agile software. The appendix regarding functional specifications has been removed and the concepts moved into the more general "Requirements Specifications" appendix.

System requirements should explicitly cover the controlled business process. Documents to be produced should be dependent on the system impact, complexity, novelty. The life cycle model for Category 4 software has been slightly modified, still maintaining the same basic principles.

For robot systems this may imply a simplified approach to system documentation. In case validation of the system is necessary, the definition of system requirements is still required and should cover the process, system functionality and technical aspects. As a suggestion, technical and functional aspects can be documented using the standard documentation of the system manufacturer, while GxP critical aspects still require evaluation and proper management / testing under the end user responsibility.

1.3.5 Updates in Appendix on electronic production of records

Cloud-based technology and blockchain have been considered. The appendix on Electronic Production Records clarifies new expectations around electronic records, electronic signatures, and audit trails.

Detailed description of data flows and supporting systems can help understanding the requirements for supervisory systems like MES, SCADA used also in robotics applications.

1.3.6 New appendix about blockchain and distributed ledger technology

The Second Edition of GAMP 5 contains a new appendix taking blockchain and ledger technology into account.

1.3.7 New appendix about AI and machine learning

The new Guide acknowledges the increasingly significant role played by artificial intelligence (AI) and Machine Learning (ML), and adds a new appendix to deal with the topic.

1.3.8 New appendix about modern infrastructure and IT services

The replacement of paper with automation and AI is increasing in the life science sector. The Second Edition contains a new appendix outlining the modern GxP infrastructure, and how new digital tools should be implemented and applied.

Multiple appendices have been updated to reflect the modern ITIL (Information Technology Infrastructure Library) approach to software development and IT services, and to clarify links between key areas like change and incident management.

IT Infrastructure is often involved in robotic applications, and GAMP provide useful guidance to manage GxP compliance implications.

1.4 FDA (draft) Guide: Computer Software Assurance (CSA)

A new FDA guidance document has been finally published by FDA in September 2022, after almost 10 years of conceptual development and pilot applications: "Computer Software Assurance for Production and Quality System Software" – Draft Guidance for Industry and Food and Drug Administration Staff.

The current status is a draft version for comments and is officially targeted to Medical Devices (only software used to support manufacturing processes and Quality System, not software embedded in the device). The main objective of the guide is to improve software quality while reducing validation efforts, and it is based on the management of risks for the process (where the system impacts on the safety of the products delivered to the patients).

The change of paradigm described in the new FDA guide is however potentially suitable also for other regulated areas, such as pharmaceutical manufacturing, though this is not (yet) officially supported.

The FDA guide distinguishes only two levels of criticality:

- **High process risk**
- **Non-high process risk**

One of the improvement areas is in the testing of the system. Different test approaches are provided, divided in two major categories:

- **Scripted Testing** (suitable for "high process risk" software features, functions, or operations)
- **Unscripted Testing** (suitable for "non high process risk" functions).

Note: The main concepts of the CSA initiative have been already covered in the GAMP 5 2nd Edition and therefore made applicable in all Life Sciences regulated software applications. Further details about this new approach are in the Testing section in Chapter 2 - Validation Approach.

1.5 Regulations in force

1.5.1 Validation

Computerized systems used in regulated industries such as pharmaceuticals must be validated. The terms "validation" and "verification" are well known concepts in software engineering. In essence "validation" means demonstration of the suitability for specific requirements, while the term "verification" indicates the demonstration of the results obtained in a specific step of the software development (e.g. verification of the expectations in a single phase or stage).

General validation concepts, and the required documentation, can be found in various regulatory documents, such as:

- EU GMP Annex 15 (Qualification and Validation)
- EU GMP Annex 11 (Computerized Systems)
- FDA 21 CFR Part 210 and 211 (US GMP for finished products)
- FDA 21 CFR Part 11 (Electronic Records and Electronic Signatures)

Other sectors (such as Medical Devices, Blood Product etc.) are regulated by different regulations, with similar requirements.

1.5.2 GAMP approach to validation

Since the publication of the GAMP 5 Guide in 2008, the term "validation" has been replaced with the more general concept of "verification". In other words what really matters is the entire process of verification of the specifications, including the higher-level requirements.

With this definition in mind, GAMP states that the software verification can be performed in a combination of different approaches (see below).

2 GxP Compliance and Validation Approach

2.1 Application of the new GAMP and FDA approaches to AMR validation

The new GAMP Guide 2nd edition and the draft FDA CSA guide can help simplifying the validation process, in both main steps:

- Specification phase (i.e. the management of the necessary documentation)
- Verification phase (i.e. the execution of the tests necessary to demonstrate the suitability for the purpose of the system).

Suggested simplifications require significant support from the suppliers of the system, with a contribution from the component manufacturer (Omron).

2.2 General aspects

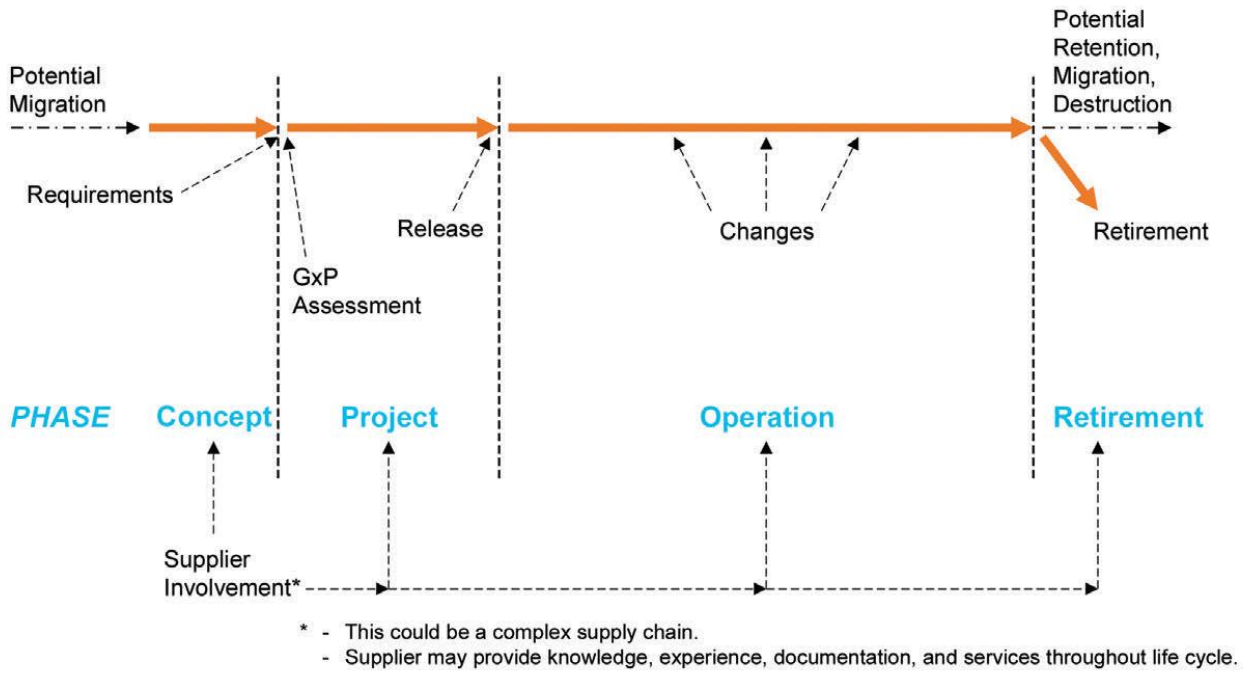
> 🕮 *Typical computer validation approaches, including the relevant activities and documents, are covered in greater detail in the OMRON Vision Systems White Paper document [32], largely applicable also to mobile robots. It is therefore recommended to read the reference document to get the basis of the approach.*

GAMP guidance documents are a valuable reference to manage validation of the entire robot system, and the recent second edition [15] helps increasing efficacy and effectiveness.

The main objective of validation remains demonstration of the suitability of the system for the intended use, with a specific focus on the critical aspects to protect the patient safety, product quality and data integrity.

Life cycle

The robot system lifecycle, like any other computerized system, can be represented as a sequence of phases, which are well represented by the GAMP model:



* Source: GAMP 5 Second Edition, © ISPE GAMP 2022.

The main phases are the project phase and the operational phase, also mentioned in some regulations (EU GMP Annex 11).

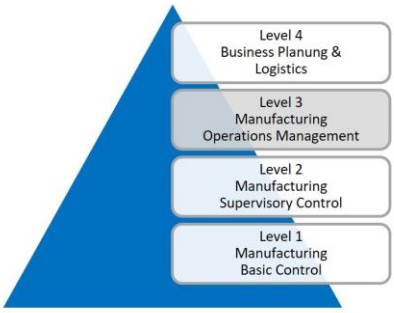
System validation should be performed during the project phase, before the system release (Annex 11 requirement). Authorization for use in regulated industries (system go-live) can be granted by the regulated company only after the validation.

Additional validation activities may be required during the operation phase, for example to validate system changes.

2.2.1 Typical architecture of a robot system - Items to be validated

The robot system architecture may be conveniently structured into different levels, using the well-known automation pyramid model from ISA-95.

- Level 0: Physical manufacturing process (not shown here)
- Level 1: Equipment (mechanical, electrical, and pneumatic components) and relevant control units
- Level 2: Robot control system (including hardware & software)
- Level 3: External systems (such as a supervisory system)
- Level 4: ERP system (not applicable here)



LEVEL 1 (Manufacturing Basic Control)

Autonomous Mobile Robots (AMR) belong to level 1. These units can be thought as a combination of mechanical and electrical parts, governed by a suitable software incorporated in the mobile unit (firmware). AMR usually have an "AMR top module" part necessary to fulfill specific tasks when the AMR is located in one of the goal positions. Control and coordination of the two parts may require an additional (mobile) control unit.

Mobile Manipulators (MoMa) still composed of two parts. However, those have a more complex structure consisting of a "Cobot" (collaborative robot) on top of an AMR. MoMa may include a more complex local controller.

- **Autonomous Mobile Robots** (Level 1) include the Mobile Robot units and may also include manipulators installed on top of the mobile unit (MoMa). Each part of the robot has its own hardware and software (firmware), that need to be coordinated together.
- **MoMa** May also include a more complex local controller (MoMa). Both parts are controlled by OMRON supplied software and connected with the rest of the world with suitable interfaces (e.g. connection to the company LAN).

LEVEL 2 (Manufacturing Supervisory Control)

Mobile units exchange data with other system components used to issue commands, monitor operations, or coordinate system components tasks. These components make use of tablets, smartphones, mobile and/or fixed computer systems, and belong to level 2. A typical example of a standard component is the Omron's **Fleet Manager**.

Auxiliary computer systems are used to configure the system during the project phase, or to change the operation of the system during the operational life of the robot system, using appropriate hardware and software tools. They are not strictly part of the operational architecture. Configuration stations are also located at level 2 of the general architecture. Software used for configuration is provided by OMRON.

LEVEL 3 (Manufacturing Operations Management)

External computer systems like **SCADA, MES, WMS** etc. are often used to collect and store data in the long term, or to support recipe based operation and configuration of the system. These units are normally part of a wider automation layer, are programmed by other suppliers, and belong to level 3.

Level 3 units are mentioned in this document for the sake of completeness but are under the responsibility of the system integrator and out of the scope of Omron. Omron provides the necessary interfaces and supporting tools for linking the Fleet Manager with any level 3 system. In more complex systems the system integrator provides a middleware which is used for more convenient data handling and may extend functionality.

LEVEL 4 (Business Planning & Logistics)

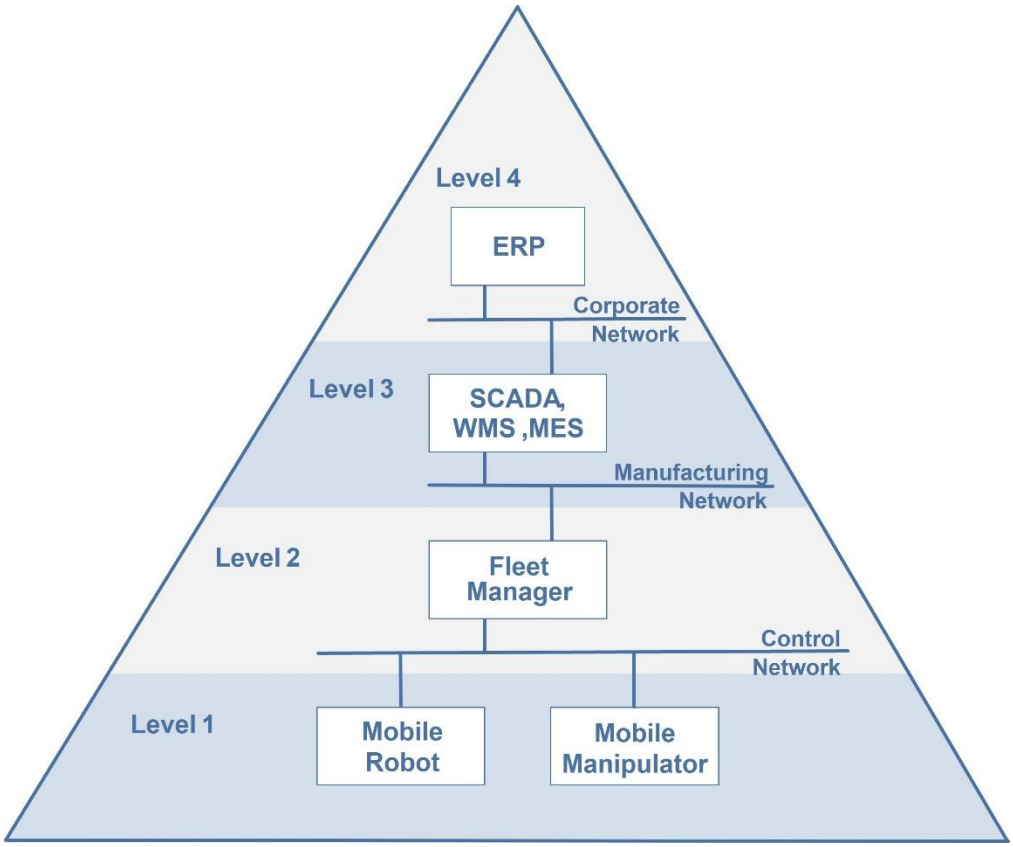
It is worth noting that level 4 systems, like **ERPs**, may be connected to lower-level components, but this scenario is not of interest in this document.

2.2.2 IT INFRASTRUCTURE

In addition, a typical robot system architecture includes (portions of) the company **IT infrastructure**, used as a support platform for the various system components.

Infrastructure may include LAN/WAN components necessary to connect all devices (e.g. router, switches, modems, etc.), backup devices, information security devices and relevant services and procedures. Many modern level 3 applications are based on infrastructure, with a client-server architecture.

Infrastructure hardware and software components are generally managed and qualified by the end user company, often with support of many different suppliers.



The picture shows a simplified automation architecture for a robot system with the levels according to the ISA-95 pyramid and the layers of the different networks.

A proper approach to robot system validation should include a clear definition of the entire architecture, and a list of components involved with operation and any supporting tools. Support systems are in general less critical and may fall into a low impact category that doesn't require validation / qualification. Data storage and long-term retention, where necessary, is normally performed with external systems such as SCADA.

The entire robot system, depending on the application area, the criticality of the process and system criticality, may require validation according to the applicable regulations. For example in pharmaceutical industries:

- In Europe Annex 11 (Computerized Systems) and Annex 15 (Qualification and Validation) could be both applicable since the robots include elements beyond computer hardware and software.
- In US the FDA 21 CFR Part 211 is the reference. Part 11 may be applicable or not, depending on the criticality of the records (i.e. the existence of "Part 11 Records") and the use of electronic signatures ("Part 11 Signatures"). In general, only external systems maintain Part 11 Records and may also use electronic signatures.

> 🕮 *Please refer to the Omron Vision System WP [32] for a summary of the typical applicable regulations for a generic automation system, and a detailed definition of Part 11 records and signatures.*

The IT infrastructure may also require qualification (according to EU GMP Annex 11). Infrastructures are shared platforms, often very complex, that support many different applications and systems (GxP and non-

GxP). The new GAMP Guide provides updated guidance on infrastructure qualification, that is outside the scope of this document, and is usually managed as a separate activity from the validation of GxP applications.

Components subject to validation / qualification should be identified with a risk assessment at system level, during the initial steps of the system life cycle (concept or project phase). A rationale for the need of validation and the chosen approach is typically documented in the assessment report or in the Validation Plan.

It should be noted that many mobile robot pharmaceutical applications do NOT generate data with high GxP criticality (Part 11 records), so there may be little or no need to officially retain them for GxP compliance. When a low system and/or data criticality can be demonstrated with a risk assessment, the entire validation approach can be greatly simplified (as suggested by GAMP 2nd Ed. and FDA CSA), and data integrity requirements can be relaxed. For example, audit trails may be not strictly necessary, and compliant electronic signatures not required (as there are no Part 11 signatures).

A GxP system impact evaluation, with a suitable risk assessment is the recommended way to establish and document the overall system criticality and the need to validate the system, including any data integrity requirements.

See the compliance consideration to examples 1 and 2 for further details.

2.2.3 Hardware and Software category

GAMP 5 categories for hardware and software are also applicable to AMRs, and remain nearly unchanged in the 2nd Edition, apart from some minor details.

> 🕮 *Please refer to the Omron WP Validation of Vision Systems [32] for details about the various GAMP categories.*

A few updated comments regarding GAMP categories (from GAMP 2nd Edition):

- *Computerized systems are generally made up of a combination of components from different categories; the categories should be viewed as a continuum.*
- *The software category is just one factor in a risk-based approach; the life cycle activities should be scaled based on the overall GxP impact, complexity, and novelty of the system (derived from the criticality of the business process supported by the system).*
- *Software categories still bring benefit in deciding the rigor of supplier assessment and also when judging the probability of a failure or defect occurring in a system.*

OMRON mobile robots' components contain only standard hardware (Category 1) and standard/configured software (category 3 and 4).

OMRON standard software is highly configurable and can be used to implement a wide variety of applications, in many different industry sectors.

There is generally no need to develop custom software components (Category 5) to implement a typical robot system. However, in some cases custom hardware and/or software elements can be required to fulfill specific intended uses, using third party components – provided by the system integrator. These components should be classified and adequately managed during validation (see Example 2 - MoMa).

It should be noted that most systems contain components of multiple categories, starting from category 1 (operating systems, databases, supporting tools, IT services). The software categories can assist in understanding the system structure; however, the life cycle activities should be always scaled based on risk, complexity, and novelty, and supported by critical thinking.

2.2.4 Stakeholders

During the implementation of a robot system application, several stakeholders are normally involved:

- **Robot Components manufacturer** (OMRON)
- **System Integrators / OEMs** (assembling/configuring a robot system using standard OMRON components, and/or supplying any other optional mechanical, electrical and/or software components)
- **End User** (i.e., the regulated company)

As for any computerized system used in regulated environments, the ultimate responsibility for the validation of the robot system stays with the end user. However, the supplier of the solution - and to some extent the manufacturer of the components - plays a role and can contribute to a successful result. GAMP strongly encourages suppliers' involvement and helps addressing roles and responsibilities.

Validation requirements increase with system complexity, especially when novelty elements / custom components (supplied by an OEM or system integrator) are present.

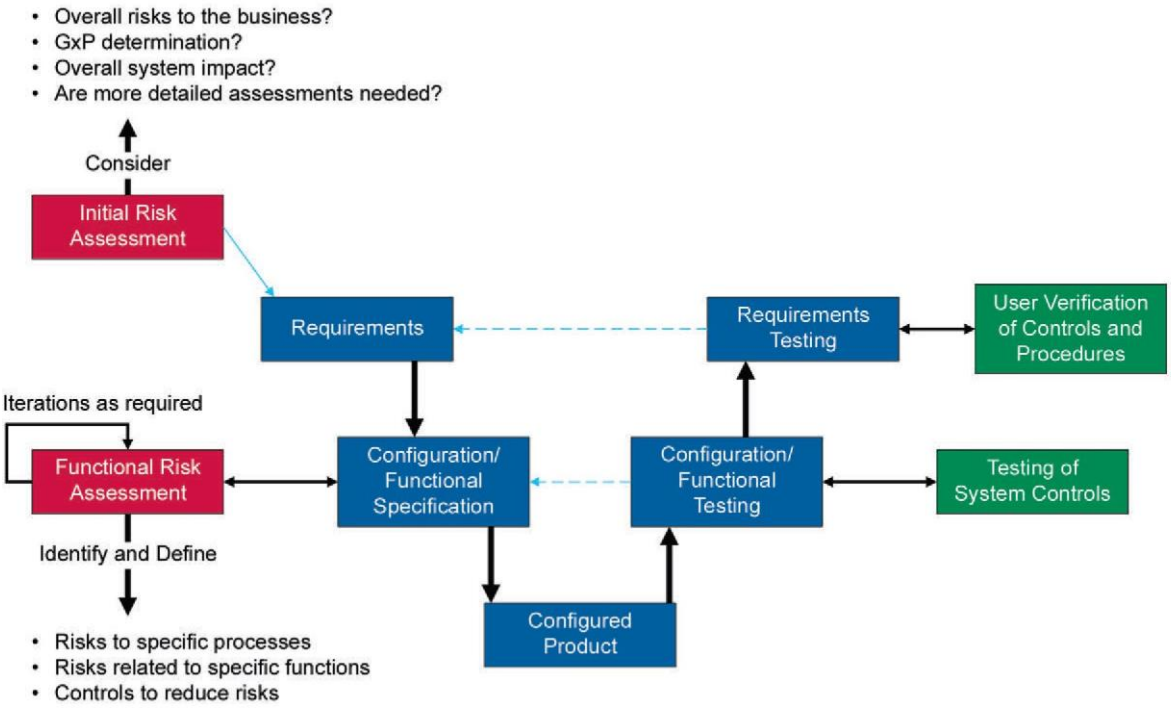
This will be further clarified in the examples and the related compliance considerations.

2.3 Life Cycle for configured software (GAMP® category 4)

2.3.1 Risk-based Validation Life Cycle

"For a typical Category 4 product it may be necessary to carry out an initial risk assessment to determine whether the system is GxP regulated and to understand the overall system impact, followed by one or more detailed risk assessments as the system specification is developed. However, for some systems it may be possible to cover all risks in the initial assessment".

For a typical Category 4 software (configured components), the project phase validation life cycle can be described as follows:



* Source: GAMP 5 Second Edition, © ISPE GAMP 2022.

2.3.1.1 Roles and responsibilities

The above model describes the validation lifecycle, from the end user point of view. The development life cycle can be significantly more complex and involves the design and manufacture of the system

components on the supplier's side. The development life cycle usually covers years of software development and the release of several software versions on the market.

Requirements definition remains a responsibility of the end user, while Configuration/Functional Specifications are typically a responsibility of the suppliers (software developers and /or system integrators and component manufacturer).

Likewise, requirements testing remains typically a responsibility of the end user, while Configuration/Functional Specifications testing can be largely supported and documented by the suppliers (especially system integrators, who have a good understanding of the specific system intended use).

System Controls and Company Procedures necessary to ensure the fulfilment of the intended use should also be considered during validation as an integral part of the risk management process.

Appropriate suppliers' qualification is required when GxP components or services are supplied.

Standard documentation provided by the component manufacturer (OMRON and any other third party) can be useful to support validation activities but is generally less critical than specific documentation that describes the project and the application.

TYPICAL RESPONSIBILITIES:

Activity / Document	End User	System Integrator	AMR Component Manufacturer	Comments
Requirements	■	■	-	
Initial Risk Assessment	■	■	-	
Configuration/Functional Specifications	■	■	■	OMRON supply standard technical documents
Functional Risk Assessment	■	■	-	
Configuration/Functional Testing (incl. testing of system controls)	■	■	-	OMRON support tools can be useful to perform tests.
Requirements Testing (incl. verification of controls and procedures)	■	■	-	

Legend:

- ■ Main responsibility /
- O Significant contribution / Approval
- ■ Support / Contribution
- \- No direct responsibility, nor support

Suppliers' responsibility increases significantly when custom components are included in the application, and a different life cycle is required for such components (GAMP Category 5).

2.4 Validation Documents

2.4.1 General aspects and assumptions

The documents mentioned in this section refer to the validation of the robot system computer systems.

Supplementary documents may be required to properly describe and qualify / validate the rest of the system (e.g. mechanical, electrical, or pneumatic components) and the controlled business process.

Additional documents may also be required to demonstrate compliance with other regulations, such as the safety of the operators. This may include adequate certifications (e.g. EU mark according to the EU Machinery Directive, or a demonstration of compliance with ISO 10218 Robots and robotic devices — Safety requirements for industrial robots — Part 1: Robots. Further requirements may apply to the entire Robot System, such as ISO 10218-2 Robots and robotic devices — Safety requirements for industrial robots — Part 2: Robot systems and integration. These topics do not regard GxP compliance and are beyond the scope of this document.

In this paper a typical case of a configurable system is assumed (category 4), with some advice in case custom hardware or software is also included. More documents may be required for a system containing custom software (category 5) e.g. a robot system that includes nonstandard elements developed by a system integrator / OEM).

GAMP 2nd Edition suggests a modern approach to manage validation in an efficient manner and reinforces the principle that documents should be adequate for the overall system GxP impact, complexity, and novelty of the application.

Standard documents available from the manufacturer of the various components can be used as a reference and further simplify the documentation.

2.4.2 Typical validation documents

A typical list of essential validation documents:

- Requirements Specification
- Validation Plan
- Technical Specifications (Functional / Configuration / Design)
- (Quality) Risk Assessment
- Test documents (test protocols / scripts, reports, etc.)
- Validation Report

(see § 3.5 “Validation documents” for a more complete list of possible documents, based on system impact and complexity).

2.4.3 Specifications

User Requirements Specification (URS) is a document expressly mentioned in EU GMP Annex 11 and Annex 15, and is considered therefore a regulatory requirement. It is a document typically produced by the end user to describe the intended use in a structured manner. URS if often prepared in cooperation with system suppliers.

Validation Plan describes the validation activities that are deemed necessary.

Functional Specifications can also be required to describe the technical behavior of the system. Technical documents are generally prepared by the system’s suppliers and then reviewed and approved by the end user.

Configuration Specification System configuration is an often-overlooked area in the documentation. However, for very common Category 4 software components it’s essential to document how standard system elements have been adapted to fit the specific requirements of the end user. Generic standard

documentation can be very useful and reduce efforts, but it's not enough to document and demonstrate the actual intended use.

Design Specification. Design documents are required for category 5 software (ad-hoc development). This is rarely necessary but may be the case for custom made AMR top modules / Cobots or custom level 3 software e.g. middleware.

These documents may be sometimes combined together, e.g. preparing Functional & Design Specifications.

2.4.3.1 Risk Management

Initial Risk Assessment should cover system-wide functional aspects and data, to establish the need for a validation and a more detailed functional and data risk management.

Complex and/or more critical systems require detailed analysis of system functionalities, and the definition of critical data (if any) that need to be controlled, recorded, and retained for compliance with the GxP regulations.

Risk Assessment is the responsibility of the end user, but very often the supplier can offer support.

2.4.4 Test Documents and reports

Test documents. Testing can be performed in different ways, with different kinds of documents (e.g. Scripted / Unscripted Tests, see below). Tests require an adequate level of reporting. See the section "Testing" for details.

Testing is in general a responsibility of the end user, but very often the supplier can offer significant support. Some tests can be entirely performed by the supplier, provided that results, reports and required evidences of testing are made available to the end user.

Traceability Matrix. This is a useful document that explains connections between the requirements, the specifications and the test. It demonstrates that all (critical) requirements have been actually implemented in the system and verified with appropriate testing. Requirements traceability is an Annex 11 requisite.

Validation Report. Describes the actual validation activities performed, the documents produced, tests performed and their results (including anomalies) and in general documents adherence to the Validation Plan (or deviations from it).

2.5 Other topics of interest for validation

2.5.1 Suppliers Quality System (OMRON and direct supplier)

OMRON is a global organization operating worldwide governed by Quality System(s) in all areas of design, manufacturing and servicing. Certifications of the Quality systems are available online and can also be requested from the OMRON's local representative if necessary.

System integrators/OEM's information about their quality systems can be necessary in case of GxP critical applications and should be requested to the suppliers during their evaluation / assessment, preferably before issuing purchasing orders.

Chapter 5 covers in more details the Omron Quality Management System.

2.5.2 Procedural aspects

For GxP critical applications, all stakeholders should have adequate Standard Operating Procedures (SOPs) in their own quality system that cover development, configuration, as well as usage, management, maintenance, and support of the system.

Typical SOPs necessary to cover these topics may include:

- Software Development
- System Design and configuration
- Usage of the system (setup, operation, monitoring, incident management, etc.) based on actual functionality.
- Management (e.g. Users administration and security management, data integrity including backup/restore, etc.)
- Servicing and Maintenance (change control, configuration management, etc.)

Users training should be ensured and evaluated during validation, especially for critical applications.

2.5.3 Roles and responsibilities

Roles and responsibilities during the life cycle are quite different:

Activity / Document	End User	System Integrator	AMR Component Manufacturer	Comments
Software Development process	–	–	■	Can be assessed during validation (e.g. White Paper, certificates, etc.)
System Design and configuration	⭘	■	◘	OMRON can provide support to system integrators / OEMs
Usage of the system (setup, operation, monitoring, etc.) based on actual functionality.	■	–	–	–
Management (e.g. Users administration, backup/restore etc.)	■	◘	–	–
Servicing and Maintenance (change control, configuration management etc.)	■	◘	◘	OMRON technical support can be involved in case of software upgrade.

Legend:

■ Main responsibility

⭘ Significant contribution / Approval

◘ Support / Contribution

– No direct responsibility, nor support

2.5.4 Cyber Security

Information security is quite important for both the business and GxP compliance, and requires adequate measures during the life cycle:

- Proper design of the system software in critical components (e.g. designed to provide suitable users access levels and privileges)
- Proper system architecture (e.g. backup systems, presence and setup of infrastructure devices like firewalls, antivirus, etc.)

- Proper configuration of the system and user's profiles – including data integrity considerations (e.g. segregation of duties, limitation of administrator's privileges, etc.)
- Proper management and change control during the operation, generally covered by end user's SOPs and agreements with the suppliers. Backup/restore of critical data and business continuity procedures are also important and should not be overlooked to recover from cyberattacks.

2.5.5 Data Integrity and Retention – management of Electronic Records and Electronic Signatures

Typical AMR systems have limited GxP impact even when used in regulated applications. Therefore, in most cases data integrity requirements and system controls can be greatly simplified. Strict application of all the regulatory data integrity requirements may be not mandatory, and in some cases may be limited to business perspective only.

Robot systems can generate a significant amount of **service data**, i.e. non-GxP data that can be very useful for technical monitoring, troubleshooting, maintenance and similar activities. The opportunity to store and retain such records is purely a business choice and doesn't affect compliance.

Some GxP requirements, such as audit trails, can be unnecessary on local data, and data integrity controls could be limited to suitable configuration to ensure information security. Backup and restore of level 1 components can be managed with ordinary business practices.

Electronic Signatures are often unnecessary for level 1 and 2 components, and user management can be limited to ordinary technical controls (such as secured users' authentication at local or network level, to provide sufficient protection of system configuration and data).

Changes in system software, including configuration, can be managed at procedural level.

Initial System (GxP) Assessment is however always necessary to evaluate the global GxP impact of the entire system and the relevant data and justify the approach.

In case GxP assessment reveals a high criticality, a more stringent approach should be used for system documentation, controls implementation, testing and management during operation.

GxP data integrity requirements should be evaluated to provide adequate measures to ensure data security and long-term retention of any GxP data (e.g. transferring GxP critical data to an external system, such as a SCADA, properly validated).

See examples 1 and 2 for more specific application details.

2.6 Testing

Testing has always been an essential part of the validation process. The new guidelines can help reducing the efforts and manage tests with "a *least-burdensome approach, where the burden of validation is no more than necessary to address the risk"* (source: FDA CSA guide).

2.6.1 Approach to validation testing

According to GAMP 5 2nd Edition and FDA CSA draft guideline, testing may be differentiated in two broad classes, according to system components risk or criticality:

- Unscripted Testing (suitable only for low-risk functions)
- Scripted Testing (necessary for high-risk functions).

Test Type	Description	Required Records / Documents	Application scenario
Scripted	Dynamic testing in which the tester's actions are prescribed by written instructions in a test case.	- Detailed report of assurance activity - Result for each test case - Issues found and disposition - Conclusion statement - Record of who performed testing and date - Signature and date of appropriate signatory authority	**High process risk** (when failure to perform as intended may result in a quality problem that foreseeably compromises patient safety). Applicable to: - LEVEL 3 components - High GxP impact components, if any.
Unscripted	Dynamic testing in which the tester's actions are not prescribed by written instructions in a test case.	- Summary description of features and functions tested - Result for each test case - only indication of pass/fail - Issues found and disposition - Conclusion statement - Record of who performed testing and date	**Not High Process Risk** Applicable to: - Level 2 and 1 components - Medium and Low GxP impact components

Function risks and criticality should be based on the impact on the controlled business process (and therefore product quality and patient safety).

> 🕮 *Refer to the GAMP 5 Second Edition Appendix D5 "Testing of Computerized Systems" for a detailed description of Scripted / Unscripted test activities (planning, execution, and the relevant records results).*

The chosen test level should be justified with a risk assessment.

GAMP recommendations about testing:

- **Critical thinking** should be applied when planning testing efforts such that the level of effort is commensurate to the risk acceptable within the organization as defined in its policies, procedures, and plans. The regulated company determines the assurance activities based on their own need to ensure systems are fit for intended use.
- **Testing** by any means and in any part of the life cycle and in any environment (development, validation, production, DevOps, etc.) **all contributes** to finding defects and confirming the system is fit for intended use.
- The use of **exploratory testing and other unscripted techniques is encouraged**. Unscripted testing must be documented and can then be leveraged as part of the overall verification stage. Using automated testing brings benefits to test coverage, repeatability, and speed.
- Modern approaches may rely on records, information, and artifacts in **automated tools** in place of formal specification and test documentation. Either approach is acceptable, provided the information is complete, accurate, available, and adequately demonstrates that the system is fit for intended use and maintained in a validated state throughout its operational life.

Note: Unscripted tests can be performed entirely by the suppliers, provided that they produce the required records / documents. Usually test contents, like FAT and SAT are agreed between the suppliers and the end users, and the end user takes part during such tests execution.

2.7 Audit trail considerations

In GxP critical applications there are two main requirements for audit trails and other recording of changes and:

1. Changes in system configuration (audit trail of system settings and parameters)
2. Changes in production data (audit trail of master data and transactional data).

2.7.1 Changes in system configuration

There is no regulatory obligation to have a system-generated audit trail for the system settings. However, when a system-based logging mechanism is available to track configuration changes, this can simplify the change management process and provide better management. However, even audit trails alone cannot ensure a complete documentation of the change process. Some level of procedural activities is always necessary.

According to GAMP, systems configuration should be properly specified and verified during the project phase, as an integral part of the validation process for Category 4 software (see life cycle model).

Regulatory requirements (such as Annex 11 §10: Change and Configuration Management) can be satisfied with procedural means, supported by technical means to capture "snapshots" of the system configuration - before and after changes, e.g. by:

- Extraction of system configuration parameters, using built-in reporting features
- Collecting evidence of the configuration settings, using screenshots.

It's important to note that configuration changes should be carefully managed for critical components, i.e. where the specific system component handles critical-to-quality process aspects and exhibits a high process

risk. Not all components are equally important, and the definition of critical items should be done during the (initial) system assessment.

Computer software and the relevant configuration should be protected against uncontrolled changes with adequate measures, such as restricted access to configuration functions, and system settings back-up (to ensure a proper restore in case of system failures or malfunctions).

2.7.2 Changes in production data

Changes in production data should be carefully evaluated and risk assessed. It's convenient to distinguish two main types of production data:

- Master data (such as recipes, process parameters settings, etc.)
- Transactional data (such as historical process variables, operations performed, etc.)

The best approach to protect data and ensure compliance is to avoid process data modifications, thus avoiding the need for audit trails. This is especially feasible for critical process variables requiring historical recording.

Recipes and other process parameters settings are often modifiable by the end user, for example to process different products in the same manufacturing system. A possible approach to maintain compliance and traceability is to manage this information in a level 3 external system, such as a SCADA o MES, and upload approved recipes or settings to the robot system (level 2 and 1 components), without allowing changes to the settings on the target system.

Automation systems governed by local controllers in general are not capable of recording a lot of data and ensuring long-term retention of data. This is a common limit for PLCs and similar process control systems. When critical data exists requiring recording and retention, for business and/or compliance purposes, it's recommended to move data to an external system (such as SCADA, MES, WMS, ERP, etc.) and ensure that data cannot be modified on the source system before data transfer.

OMRON software is designed to ensure that temporary storage of data in the local systems is secure from alteration or deletion or can be protected against wrong access. Once locally generated critical data is transferred to the external storage system, it can be safely deleted in the low-level components.

Under this scenario, data integrity requirements (including long-term retention of GxP / Part 11 records) can be verified / validated mainly on the external systems, with less efforts on level 1 and 2 components.

For the sake of clarity it should be mentioned: The Fleet Manager as such has no HMI. If human intervention in the automated process is required, it must be done through the level 3 system. The audit trail that logs the operator intervention must be a function of the level 3 system.

2.7.2.1 Interfaces

When interfaces are used to transfer GxP data, they should be validated. The use of a standard software package can greatly simplify this activity. OMRON provides an "**Integration Toolkit**" for the Fleet Manager that can help the integration with external systems and data collection, as well as simplify validation of data interfaces. The toolkit is in fact a standard software, that only needs configuration for specific purposes (GAMP Category 3 to 4). See the application examples for details.

3 Application Examples

The following application examples consider only the control part of the system(s), i.e. computer systems and relevant software, not the entire equipment. Qualification of the rest of the equipment (e.g. mechanical and electrical functions / parts) is also required to achieve compliance (Annex 11), but these qualification activities are not covered here.

The examples given are illustrative only and are intended to be neither prescriptive nor exhaustive.

The autonomous Mobile Robots must be integrated into the customer environment. The required functionality could be achieved in one of two scenarios:

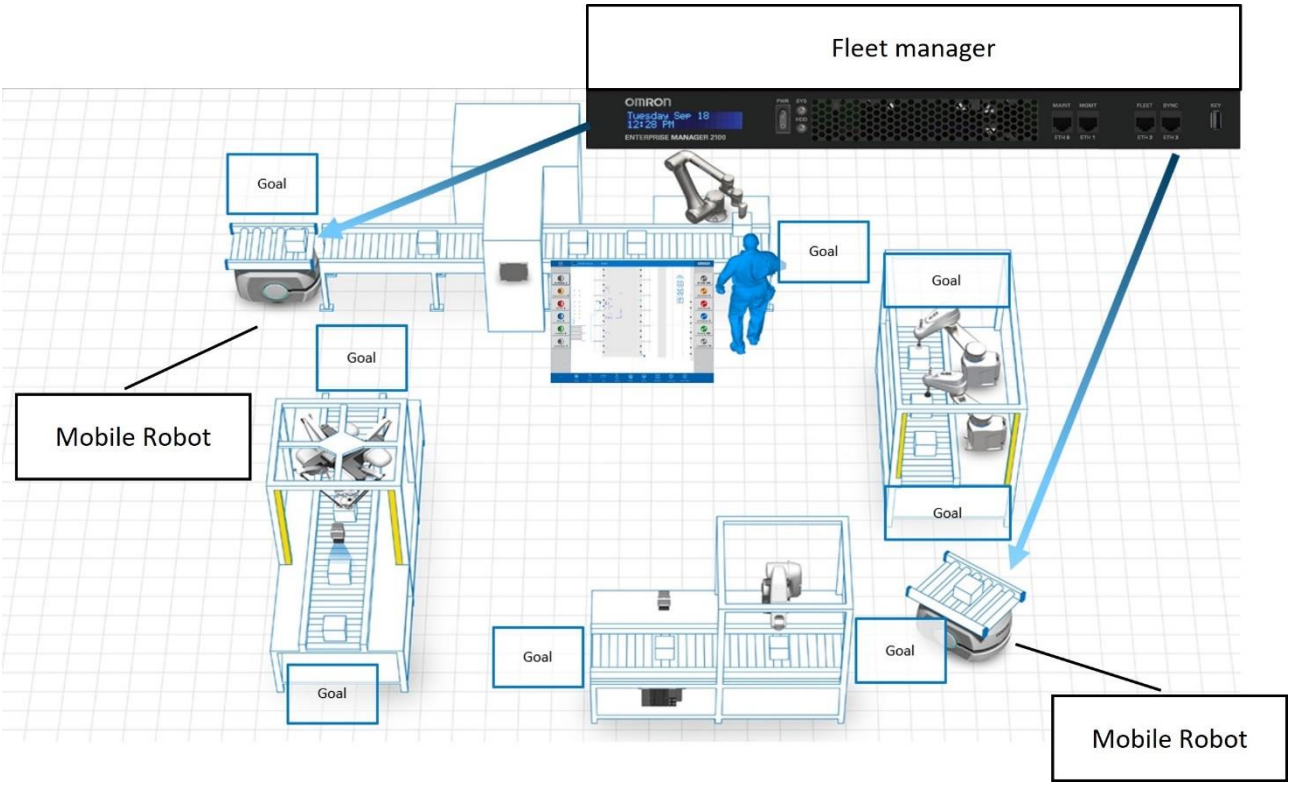
1. a fleet of Mobile Robots
2. a single or a fleet of Mobile Manipulator (Mobile Robot in combination with a Cobot).

3.1 Example 1 (Fleet of Mobile Robots)

A fleet of Mobile Robots consists of 1 – 100 autonomous Mobile Robots. All Mobile Robots in a fleet are connected to a Fleet Manager. The Fleet Manager is always necessary.

Mobile Robots will be equipped with an AMR top module according to the application needs. The AMR top modules can be the same or different on different Mobile Robots. The Mobile Robots with the AMR top module installed are considered as complete machines which are built and integrated by a machine builder / system integrator.

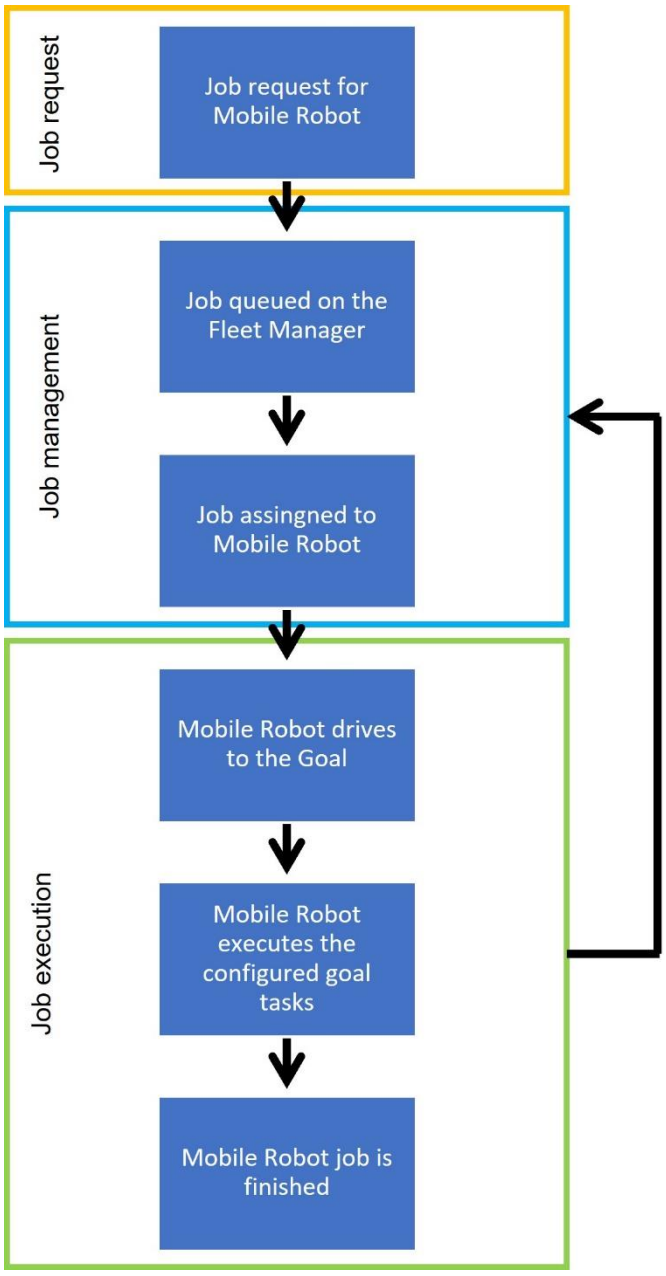
3.1.1 Application function: Performing material and product transportation



3.1.1.1 Simplified flow of operation

In a typical application, the fleet of mobile robots executes the requested jobs which are managed by the Fleet Manager.
A job can consist of one or more job segments. A segment can be either a pick-up order or a drop-off order. Each job segment is assigned to a destination on the Mobile Robot map. The mobile robot is always actively working on one order segment. When all segments of a job are completed, the job is finished.
All segments of a job must be worked on by the same robot. Jobs with one or more segments can be queued on the Fleet Manager, e.g.

- a Pickup job consists of 1 segment
- a PickupDropoff job consists of 2 segments
- a Multi job consists of more than 2 segments

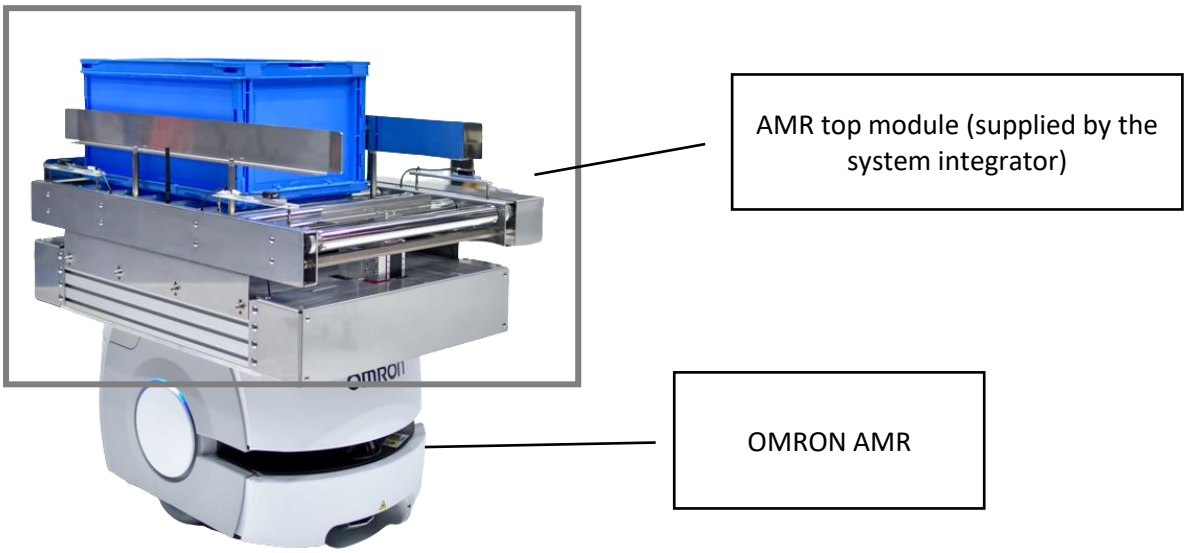


3.1.2 System Components and Architecture

The application example shows a fleet of autonomous Mobile Robot. The fleet can be mixed of different types and models of OMRON Mobile Robots.

Mobile Robot:

- The Mobile Robot consists of an OMRON AMR, LD (Light Duty) or HD (Heavy Duty) series indicated by the maximum payload and an active or passive AMR top module, e.g. box conveyor, which is added by a system integrator.
- OMRON AMR Types: LD-60/90, LD-250, HD-1500



Fleet Manager:

- The Fleet Manager, EM2100, is the central unit for configuration, job management, coordination and decision-making of a fleet of OMRON AMR.

Software:

AMR – Fleet Operation Workspace Core

The software packages listed are used to configure, operate and maintain Mobile Robot applications with OMRON AMR and Fleet Manager.

Needed

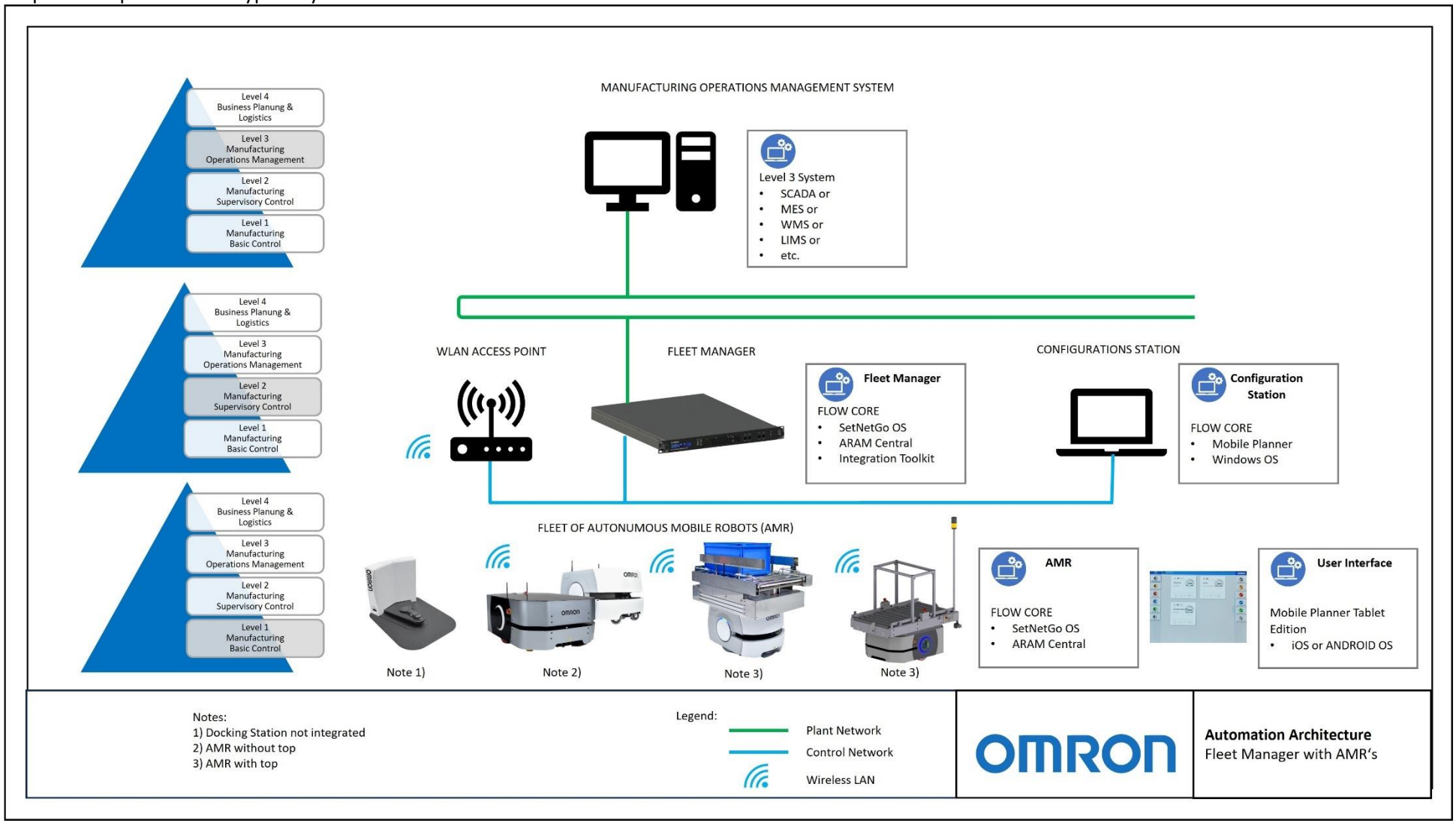
Software	Where does it run	Purpose	Used for
FLOW Core	Fleet Manager	Suite of software of the Fleet Manager	Configuration / Operation
MobilePlanner	PC	Mapping, programming, configuration, monitoring, simulation… Environment for AMR's and Fleet Manager	Configuration
SetNetGo	Fleet Manager	Operating system	Operation
SetNetGo	AMR	Operating system	Operation
Integration Toolkit	Fleet Manager	Communication methods: REST, SQL, RabbitMQ	Configuration

Optional

Software	Where does it run	Purpose	Used for
MobilePlanner Tablet	Tablets (Apple or Android)	Monitoring, Call Button. For AMR's and Fleet Manager	Operation
FLOW iQ	Fleet Manager	Analytics, dashboards, monitoring, historics, heatmaps	Operation
Fleet Simulator	Fleet Manager	Allow to configure the Fleet Manager in simulation mode	Configuration
CAPS	AMR	Increase the repeatability of the AMR	Operation

Architecture

The picture represents the typical system architecture of a fleet of Mobile Robots.



3.1.3 System Features

Main features:

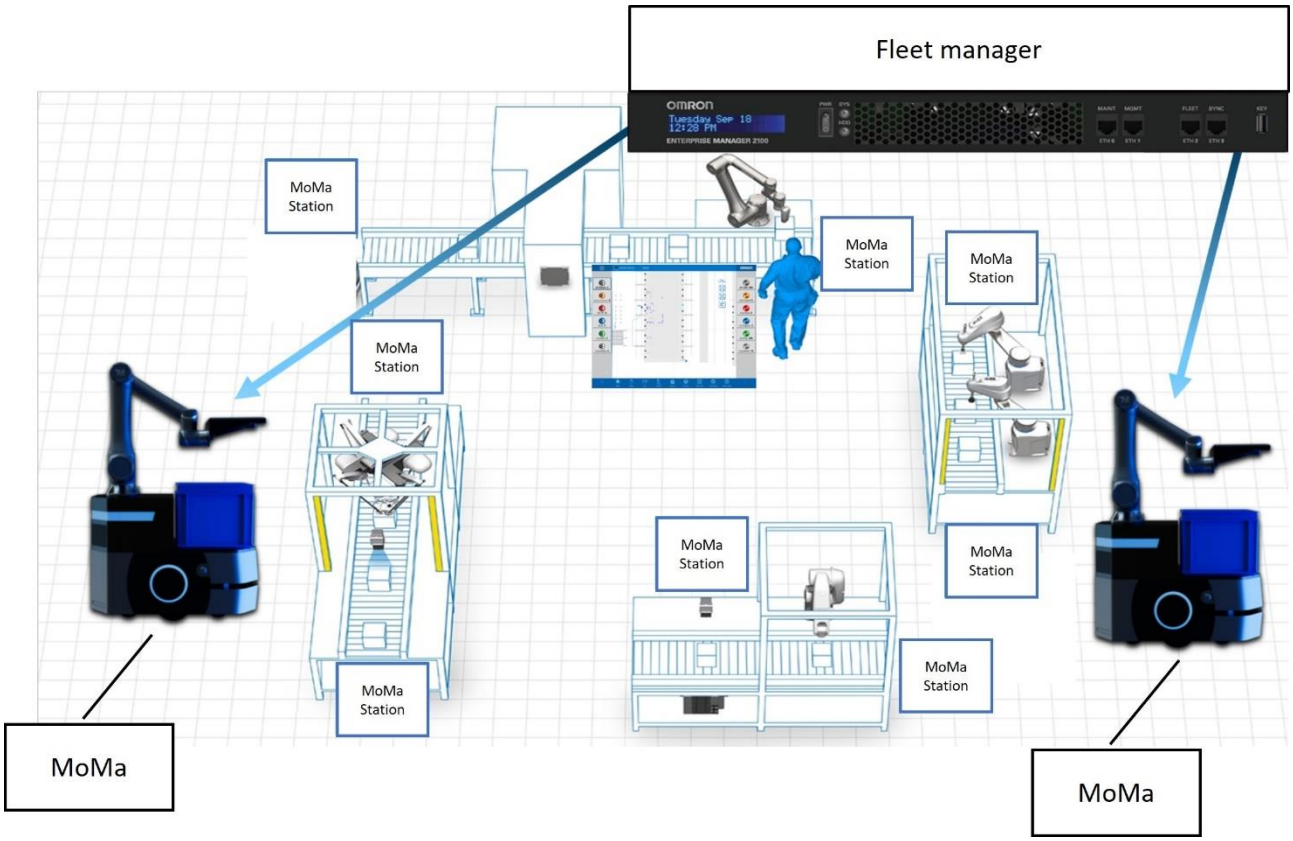
- The system is mainly intended for material and product transportation with a fleet of Mobile Robots working in the same physical environment. At the goal the selected Mobile Robot will perform the pre-defined tasks of the pick-up or drop-off job.
- Orders like pickup or drop-off jobs must be sent directly from a level 3 system, e.g. SCADA, EMS, WMS, LIMS, etc., to the fleet manager.
- The selection of the Mobile Robot to perform the pick-up or drop-off job is done by the fleet manager depending on criteria defined for the application.
- The mobile robot navigates autonomously in the environment.
- Interface between the Mobile Robot and the fleet manager is a Wireless LAN connection.

3.2 Example 2 (Mobile Manipulator – MoMa)

A fleet of MoMa consists of 1 – 100 autonomous Mobile Robots with at least a collaborative robot (Cobot) installed as AMR top module. All MoMa are connected to a Fleetmanger. The Fleet Manager is always necessary when running a MoMa.

The AMR top module of the Mobile Robots will be equipped with at least a Cobot inclusive an application specific Cobot tool. Different types of Mobile Manipulators can run in the same fleet.

3.2.1 Application function: Performing robot operations at different stations



3.2.1.1 Simplified flow of operation

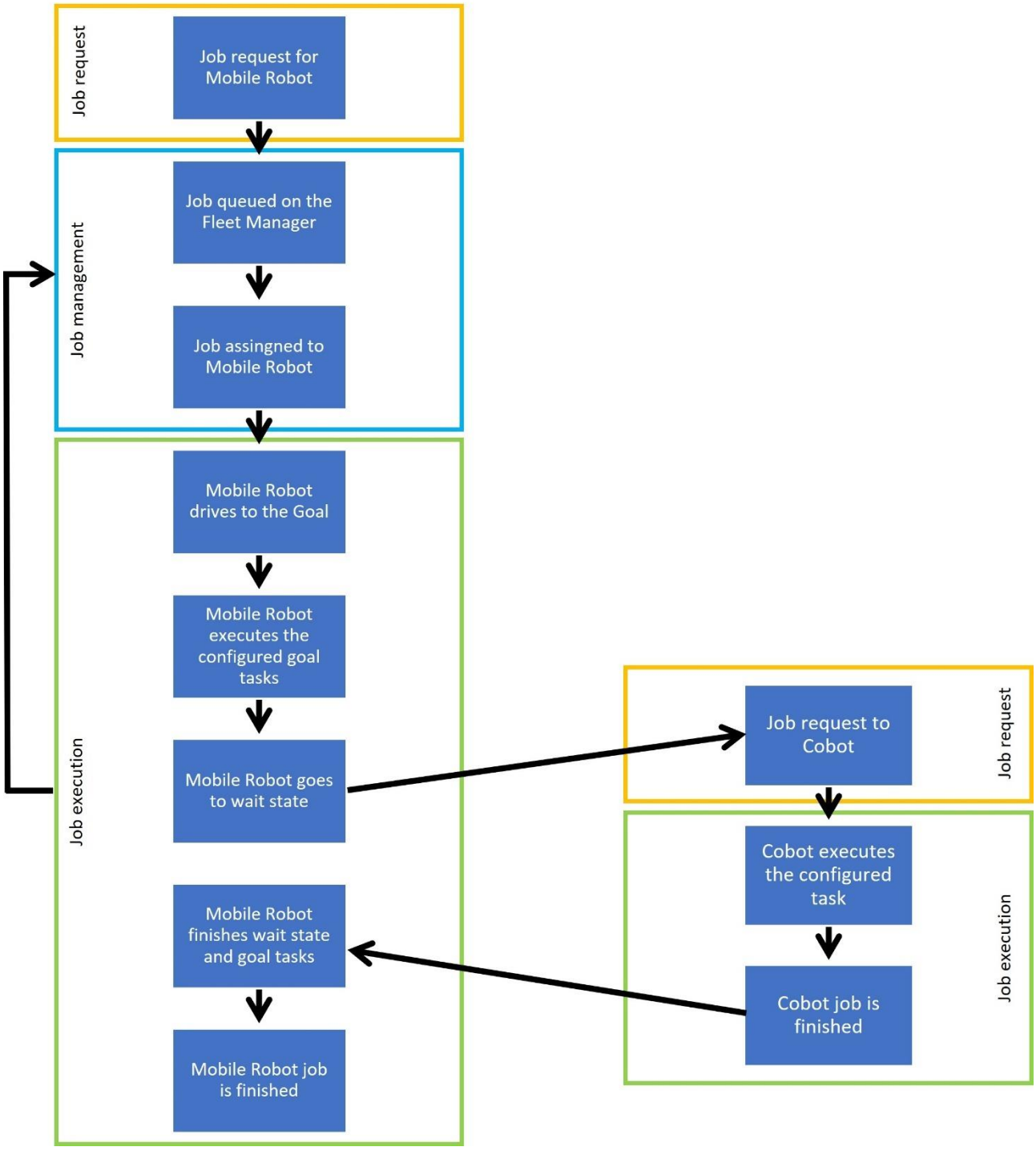
In a typical application of one or more than one MoMa , the MoMa executes the requested jobs. A job of the MoMa is split into the task the Mobile Robot must perform and the task of the Cobot. Both tasks are running in a sequential order, the Cobot stays at a safe position while the Mobile Robot drives to a goal, the Mobile Robot is in a safe state and can't drive while the Cobot is moving.

The Mobile Robot job consists of one job segment, the Pickup job, and is managed by the Fleet Manager. Each job segment is assigned to a goal on the Mobile Robot map. When the Mobile Robot arrives at the goal a pre-configured Wait task is called.

The Cobot receives the job information when the Mobile Robot has reached the desired goal and the Wait task is active. The job of the Cobot must be pre-configured in the Cobot application program and can consist of several steps of activities or product handling at the same goal. When all configured functions of the job are finished the Cobot is finished.

When the Cobot job is finished the Mobile Robot comes back from the Wait state, performs remaining tasks of the job segment. When all segments of a job are completed, the job of the Mobile Robot is finished.

When both, the job segments of the Mobile Robot and of the Cobot, are completed the job of the MoMa is finished.



3.2.2 System Components and Architecture

The application example shows a fleet of MoMa. The fleet can be mixed of different types and models of OMRON Mobile Robots.

Mobile Robot:

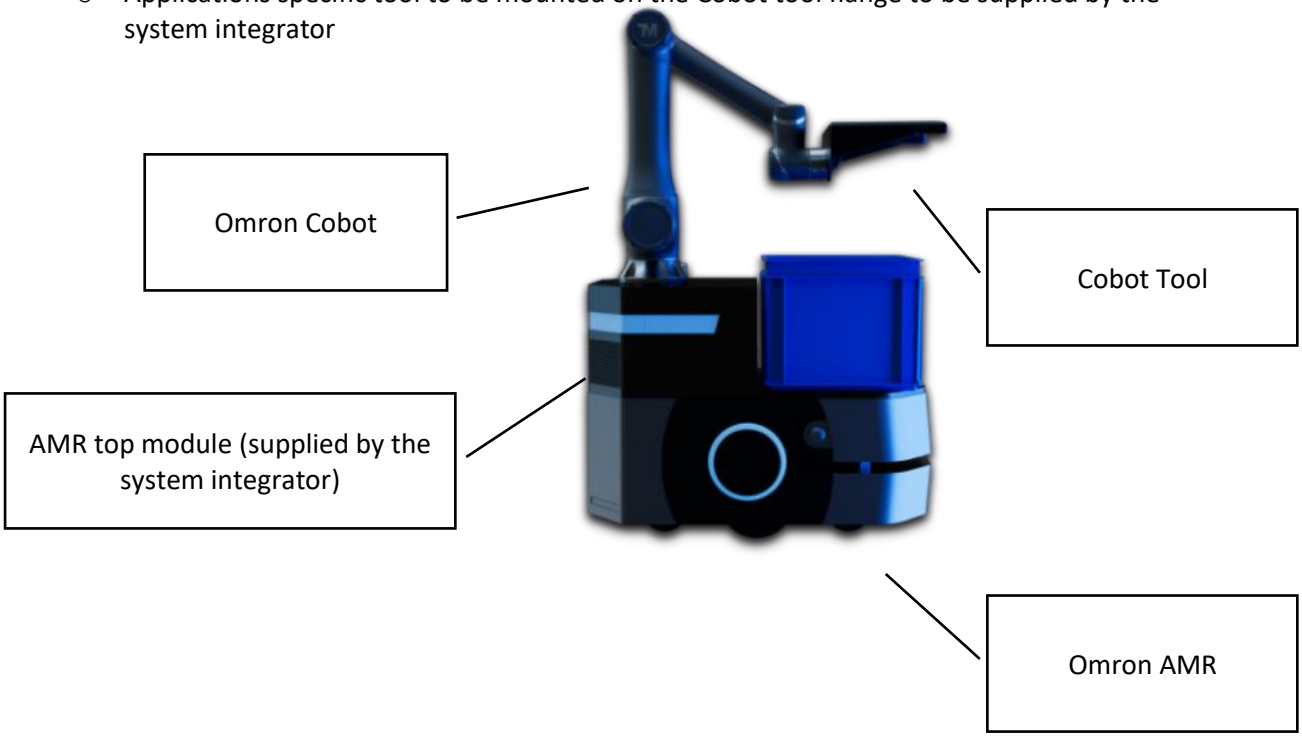
- The Mobile Robot consists of an OMRON AMR, LD (Light Duty) or HD (Heavy Duty) series indicated by the maximum payload.
- OMRON AMR Types LD-60/90, LD-250, HD-1500

Cobot:

- The following OMRON Collaborative Robots of the TM series can be used

Type	Reach (mm)	Payload (kg)
TM5-700	700	6
TM5-900	900	4
TM12	1100	12
TM14	1300	14

- Cobot Tool
  - Applications specific tool to be mounted on the Cobot tool flange to be supplied by the system integrator



Fleet Manager:

- The Fleet Manager, EM2100, is the central unit for configuration, job management, coordination and decision-making of a fleet of OMRON AMR.

MoMa Safety Controller:

- A Safety Controller which is built into the AMR top module is required for safety related interlocks between AMR operation and Cobot operation

Software:

The software packages listed are used to configure, operate and maintain MoMa applications with OMRON AMR, OMRON Cobots and Fleet Manager.

Needed

Software	Where does it run	Purpose	Used for
FLOW Core	Fleet Manager	Suite of software of the Fleet Manager	Configuration / Operation
MobilePlanner	PC	Mapping, programming, configuration, monitoring, simulation… Environment for AMR's and Fleet Manager	Configuration
SetNetGo	Fleet Manager	Operating system	Operation
SetNetGo	AMR	Operating system	Operation
Integration Toolkit	Fleet Manager	Communication methods: REST, SQL, RabbitMQ	Configuration
TM Flow	Cobot Controller	Cobot Operating System	Operation
TM Flow	Laptop	Cobot Application Configuration	Configuration

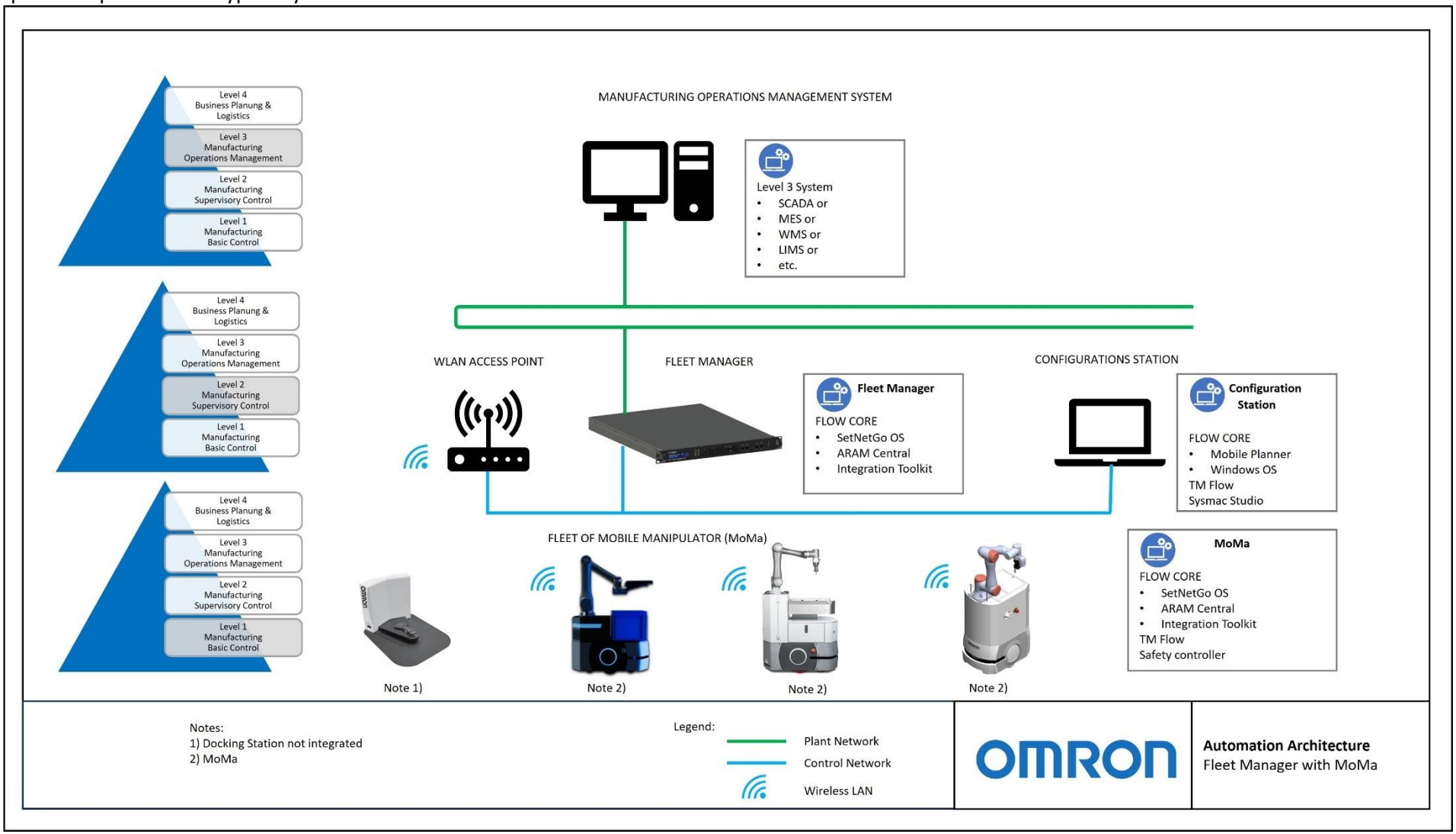
Sysmac Studio	Laptop	Safety Controller Configuration	Configuration

Optional

Software	Where does it run	Purpose	Used for
MobilePlanner Tablet	Tablets (Apple or Android)	Monitoring, Call Button. For AMR's and Fleet Manager	Operation
FLOW iQ	Fleet Manager	Analytics, dashboards, monitoring, historics, heatmaps	Operation
Fleet Simulator	Fleet Manager	Allow to configure the Fleet Manager in simulation mode	Configuration
CAPS	AMR	Increase the repeatability of the AMR	Operation

Architecture

The picture represents the typical system architecture of a fleet of MoMa.



3.2.3 System Features

Main Features:

MoMa

A MoMa consists of two 2 main elements:

1. **Mobile Robot**
    - The system is mainly intended for material and product transportation with a fleet of Mobile Robots working in the same physical environment. At the goal the selected Mobile Robot will perform the pre-defined tasks of the pick-up or drop-off job.
    - Orders like pickup or drop-off jobs must be sent directly from a level 3 system, e.g. SCADA, EMS, WMS, LIMS, etc., to the fleet manager.
    - The selection of the Mobile Robot to perform the pick-up or drop-off job is done by the fleet manager depending on criteria defined for the application.
    - The mobile robot navigates autonomously in the environment.
    - Interface between the Mobile Robot and the fleet manager is a Wireless LAN connection
2. **Cobot**
    - The Cobot's job to perform a specific robot task must be sent directly from an external system, e.g. SCADA, EMS, WMS, LIMS, etc., to the cobot controller when the mobile robot arrives at its destination.
    - The Cobot will perform the pre-defined actions at the goal.
    - Interface between the Cobot and the level 3 system is a Wireless LAN connection via the AMR.

- The MoMa is equipped with a safety controller to connect the safety systems of the Mobile Robot and the Cobot.
    - The Mobile Robot will only drive if the Cobot is in a specific home position. The home position of the Cobot is checked by a safety switch.
    - If the Cobot is not in the home position the Mobile Robot is in an Estop state.

3.3 Life cycle activities

Activities performed during the system life cycle are very similar for Example 1 and Example 2. The main difference is in the design of the MoMa, because the manipulator (Cobot) needs specific activities for the design configuration and testing.

3.3.1 Responsibility Assignment Matrix

Activities are performed by different actors:

- End User (the regulated company)
- Suppliers (system integrators or OEM who design, supply, install, verify, maintain the system)
- Manufacturers of the components (Omron and any others)

Suppliers are generally responsible for system and software configuration of standard components.

Some suppliers, like OEMs, may also be responsible for the design of custom-made components, such as special AMR top modules or manipulators used in MoMas. Their responsibility may extend to the design of custom software (GAMP category 5) that requires additional life cycle activities, documents and testing.

Roles and responsibilities during the life cycle for a typical robot system based on standard components are summarized in the following Responsibility Assignment Matrix (RACI table).

LEGEND:

R = Responsible (Action)

A = Accountable (Approval)

C = Consulted

I = Informed

Activity	Short description of the activity	End User	System Integrator(s)	OMRON
CONCEPT PHASE				
Product – Technology - Presentation	Non – application specific demo	I	R	R
Product Training	Technical training of automation components	I	R	(R)
PROJECT PHASE				
System architecture design	Process analysis and Proof of concept of the automation	R	C	-
Quality Risk Management	GxP (process) risk assessment: impact analysis, risk control (mitigation), monitoring	R	C	-
Specifications	Definition of the automation system	C	R	(1)
	Definition of number of AMRs	C	R	(1)
	AMR top module design	C	R	(1)
	AMR task definition	C	R	(1)
Configuration	Hardware and software setup of components and application	C	R	(2)
	Fleet Manager configuration	C	R	(2)
	AMR configuration	C	R	(2)
	Mobile Robot configuration	C	R	(2)
	Mobile Robot Map Creation	C	R	(2)
	Cobot configuration	C	R	(2)
Design	Cobot Design AMR top module design	C	R	(2)
Testing (FAT, SAT, commissioning, qualification)	Mobile Robot testing: ▪ Test the Top of Mobile Robot ▪ Verification of precision at goals ▪ Verification of tasks configured at goals (electrical and mechanical checks) Test of complete process, cycle time	A	R	-

Activity	Short description of the activity	End User	System Integrator(s)	OMRON
	Fleet Manager testing - Integration testing, including interfaces (3) (4): ▪ Test of configured fleet and sub fleets of Mobile Robots ▪ Test connectivity, data exchange and operation with level 3 system (e.g. SCADA, MES, DCS or ERP)	A	R	-
System Release (go-live)	Handover Start of the tested automation process	R	C	-
OPERATION PHASE				
Data collection and retention	Data collection, long-term retention, backup, (archive)	R	-	-
Process Data Management	Changes in process data (e.g. recipes and operational parameters)	R	C	(2)
Change Management	System changes (including incident management), and revalidation as needed (based on change impact and risk).	R	C	(2)
RETIREMENT PHASE				
Data migration	Data collected during the operation life of the retired system can be migrated to a new system, archived or deleted (according to a risk assessment).	R	C	(2)
System Retirement	The old system is dismissed and removed from computerized systems inventory.	R	-	-

NOTES:

(1) OMRON can provide standard documentation.
(2) OMRON can provide technical support.
(3) Level 3 systems validation regards separate applications, quite often is applicable to a number of different automation systems, and is not covered in detail in this document.
(4) IT infrastructure qualification is usually performed separately from the validation of software applications, and is not covered in detail this document.

Other details can be found in the following section (compliance considerations).

3.3.2 Risk Management considerations

In addition to GxP risk regarding potential impact on product and patient, other possible risks in a typical robot system application include:

- Safety (eg. SIL1 requirements)
- Machine Safety
- Prevent Operation Failure (human interaction, vibration & acceleration (product), power failure)
- Environmental hazards (explosive atmosphere, contamination by e.g. dropping products, ...)
- Fire-alarm -> system behavior in case of emergency (remove from escape routes)
- Design Risk (fan, material issues, …, freight securing means according to movement)
- Wet floor
- Uneven floor
- Elevator
- Automatic door bypassing
- Cleanroom class change
- Traffic crossing
- Etc.

All these risks should be properly managed by the end user and the system integrator / OEM, by performing a HAZOP study and may require additional documentation and verifications when required by regulations other than GxP (e.g. safety for the personnel), or in force of agreements between the end user and the supplier.

3.4 Compliance considerations (including ER/ES)

The following compliance and validation considerations apply to both Example 1 (AMR fleet) and Example 2 (MoMa).

There is no fixed rule or approach: validation efforts should be based on a risk assessment of the specific system and are therefore variable case to case.

3.4.1 Overall approach to compliance and validation

GxP Critical hardware and software components should be validated or qualified, based on a risk assessment. A typical application scenario in a regulated application (such as in pharmaceutical manufacturing may require:

- **IT infrastructure** can affect the robot system operation, based on the specific architecture, and should therefore be qualified (Annex 11 requirement).
- **Level 3 components** are responsible for data collection and retention, audit trail, electronic signatures (and therefore can be subject to validation and Part 11 compliance).
- **Level 2 and Level 1 components** are typically less critical and generally do not maintain critical data in the long term. These components may generate GxP ERs (Part 11 records), but they do not maintain such records. In case GxP records are detected during the risk assessment, these records should be transferred to the level 3 components for long term storage and safe retention.

With proper system design, low-level components are not subject to Part 11 requirements and validation can be greatly simplified. It is often sufficient to qualify the more critical items – e.g. the fleet manager, with a verification of low level components (integration tests). Low level components can be tested according to common business practices (including tests like FAT, SAT or UAT).

3.4.2 Special cases

- **AMR top module** Typical applications do not have a direct impact with product quality, so ordinary business practices suffice. GxP impact should be documented with a risk assessment. In some cases AMR top modules may include a custom control unit (e.g. a PLC with custom-made software), that should be treated as GAMP Category 5 software.
- **MoMa** add a degree of complexity to the level 1 components. The activity performed by the Cobot can have a direct impact with the quality of the product and may therefore require a careful risk assessment. Additional validation activities and documents may be necessary, based on risk, up to a fully documented validation with scripted testing.
- Any **custom components** (such as non-standard AMR top modules or manipulators designed ad-hoc for a specific purpose) may require a different validation life cycle, following GAMP recommendations for software category 5, when there is a direct impact with product quality.

3.4.3 Typical GxP criticality of system components and compliance approach

Validation of the entire robot system may require different activities for the various components type. Though validation is a responsibility of the end user, suppliers may play an important (support) role:

Information for risk assessment can be extracted from this table.

Component	GxP	Typical GxP Criticality	Compliance approach	Main Responsibility
IT Infrastructure				
Servers and data storage	M	Application and Database servers (for client-server systems) Data Storage for storage and long-term retention / archiving	Qualify critical servers and storage units (incl. backup systems)	End user (1)
Network and IT security tools	L	Used to connect components (LAN, WAN) Standard hardware and firmware with specific configuration.	Qualify critical components (e.g. main switches, routers, firewalls, antivirus, etc.)	End user (1)
Clients	L	Used to perform operations. Standard hardware and software, typically noncritical.	Qualify critical components, if any.	End user (1)
IT services and tools	M	Systems and Procedures to maintain the infrastructure under control and compliance	Verify tools and procedure	End user (1)
LEVEL 3 components				
MES / SCADA / WMS etc.	H	Data Collection for long term storage and retention of GxP Electronic Records Audit trail (for ERs) Electronic Signatures (if available and actually used) Part 11 compliance	Validate applications (based on GxP criticality): typically GAMP Category 4. Verify Part 11 ER/ES. Validate interfaces with other robot system components (e.g. fleet manager). Verify applicable SOPs.	End user (1)
LEVEL 2 components				
WLAN components (e.g. Access points)	L	Connectivity services (using standard network protocols such as TCP/IP). Standard hardware and software (cat. 1 or 3)	Qualification (as part of the IT Infrastructure).	End User (1)

Component	GxP	Typical GxP Criticality	Compliance approach	Main Responsibility
Fleet Manager	M	Monitoring and coordination of mobile units Configuration (cat. 4) Interface with level 3 components	Functional Test (integrated with AMR and/or MoMa and interfaces where needed) (Unscripted testing)	Supplier
Configuration Station	L	System Configuration tool (2)	Document / capture configuration (configuration units may also be used during Functional Test)	Supplier
LEVEL 1 components				
AMR (mobile robot base)	L	Low criticality (standard hardware and software). Monitoring, coordination and configuration managed in fleet manager.	Tests against the intended use (FAT/SAT), jointly with level 2 components.	End User and Supplier
AMR top modules (other suppliers, OEM)	L M	Criticality depends on the specific application and should be evaluated with a risk assessment. May include custom hardware and / or control software (cat. 5).	Tests against the intended use (FAT/SAT), jointly with level 2 components. Unscripted validation test if medium criticality	End User and Supplier
Manipulator / Cobot (MoMa)	L M H	Criticality depends on the specific application and should be evaluated with a risk assessment. May include custom hardware and / or control software (cat. 5).	FAT/SAT Validation tests may be needed if critical (scripted or unscripted tests, based on process risk). Scripted testing required if it contains custom elements.	End User and Supplier

Comments:

(1) IT infrastructure qualification and external systems are out of scope for this document, and are an end users' responsibility. Definition of specifications and verifications is usually performed in cooperation with the suppliers.

(2) Computers used for system configuration and the relevant software tools are generally not critical (GAMP category 1) and don't require validation, as they do not play a role in the operation of the system.
However, robot system configuration is important and should be specified, documented and verified during validation.

3.4.3.1 Specifications

Based on system risk assessment (see below), specification documents may be required for compliance with GxP regulations. Specification documents may include for example:

- **Validation Plan**, describing the plan of activities to be performed during validation
- **(User) Requirements** describing the intended use of the system and the applicable regulatory requirements
- **Functional Specifications** describing the operation and functionality of the specific application case
- **Reference** (standard) technical documentation

Validation documents should describe the intended use of the specific application and its technical specifications, supported as needed by standard documents produced by the manufacturers of the various components.

3.4.3.2 Risk Management

Risk assessment is necessary to identify and manage risks:

- Overall system criticality and (GxP) process impact
- Individual components criticality and risk for the process
- Critical functions
- Critical Data
- Controls required to minimize risks

Risk assessment and required controls may be documented in a separate document for complex / more critical systems, or inside other documents for simpler / less critical systems.

📖 *See GAMP 5 Appendix M3 Quality Risk Management for details.*

3.4.3.3 Test type (Software assurance)

Testing should be performed according to GAMP recommendations, differentiated according to system components risk or criticality. See § 2.6 - Testing for details.

3.5 Validation documents

Possible list in a traditional approach for a typical robotic system, depending on system impact and complexity:

ACTIVITY / DOCUMENT	Non GxP	Simple GxP	Complex GxP
Supplier(s) Audit	-	▪	▪
Validation Plan	-	▪	▪
User Requirements Specification	-	▪	▪
Project and Quality Plan	▪	▪	▪
Functional Specifications	-	▪	▪
Configuration Specifications	-	▪	▪
Design Specifications	-	▪	▪
Quality Risk Management	-	▪	▪
Traceability Matrix (Requirements / Specifications / Tests)	-	▪	▪
User Manual	▪	▪	▪
Test Plan	-	▪	▪
FAT (Factory Acceptance Test)	▪	▪	▪
SAT (Site Acceptance Test)	▪	▪	▪
Installation Qualification	-	▪	▪
Operational Qualification	-	▪	▪
Performance Qualification	-	▪	▪
Validation Report	-	▪	▪
SOPs	-	▪	▪

-	Document / activity not required
▪	Document / activity recommended, but optional.
▪	Document / activity required or strongly recommended

The document list refers only to the parts considered in scope. External / remote systems may require additional activities and a separate set of documents.

When appropriate, individual documents may be produced for single components (and not the entire robot system).

4 Applicability of 21 CFR Part 11 to Omron Mobile Robot components

The following table summarizes Part 11 compliance requirements applicable to Omron Mobile Robot components, when used in pharmaceutical application.

It does not cover other parts, developed by the end user or system integrators (such as the equipment control system).

21 CFR part 11 requirements	Level 1	Level 2	Level 3	Type	Notes
ELECTRONIC RECORDS					
11.10 (a) System validation	■	■	■	P	
11.10 (b) Record review, inspection and copy	NA	NA	■	T/P	
11.10 (c) Records protection and retrieval	■	■	■	T/P	
11.10 (d) System access	■	■	■	T/P	
11.10 (e) Audit trails	NA	NA	■	T/P	
11.10 (f) Operational system checks	■	■	■	T/P	
11.10 (g) Authority checks	■	■	■	T/P	
11.10 (h) Validity of source of data input	NA	■	■	NA	
11.10 (i) Training	■	■	■	P	
11.10 (j) Signature policy and prevention of falsification	NA	NA	■	NA	Optional
11.10 (k) Control over system documentation	■	■	■	P	
11.30 Controls for open system	NA	NA	NA	NA	Closed system
11.50 (a) Signature manifestations & required information	NA	NA	■	NA	Optional
11.50 (b) Required controls for signature records	NA	NA	■	NA	Optional
11.70 Signature/record linking	NA	NA	■	NA	
ELECTRONIC SIGNATURES					
11.100 General requirements					
11.100 (a) Electronic signature uniqueness	NA	NA	■	NA	Optional
11.100 (b) Verification of individual identity	NA	NA	■	NA	Optional
11.100 (c) Legal notification to FDA	NA	NA	■	NA	Optional
11.200 (a) Non-biometric signature	NA	NA	■	NA	Optional
11.200 (b) Genuine use of biometrics signature	NA	NA	■	NA	Optional
11.300 (a) Maintain the uniqueness of user credentials	NA	■	■	NA	Optional
11.300 (b) Credential maintenance and periodic controls	NA	■	■	NA (T/P)	Optional
11.300 (c) Deactivation of lost or compromised credentials	NA	■	■	NA (P)	Optional
11.300 (d) Prevent unauthorized use of credentials	NA	NA	■	NA	Optional
11.300 (e) Testing of identification code devices	NA	NA	■	NA	Optional

Legend: ■ = Fully applicable; ■ = Partially or optionally applicable; NA = Not Applicable to the system (e.g. procedural requirement)

T = technical requirement; P = Procedural requirement (usually covered by a specific SOP)

Observations about Electronic Records:

- Part 11 ER requirements are generally not applicable to OMRON robot systems components, with a few exceptions (system security and ER generation). ER requirements can be fully satisfied using an external system (such as a SCADA, MES, or WMS).

Observations about Electronic Signatures:

- Part 11 ES requirements are not applicable to OMRON robot systems components. Electronic signatures are optional on Level 3 systems. In case predicate rules require record signatures, these can be implemented on paper (handwritten signatures, eventually executed to electronic records – see 11.70).

- Some ES requirements have been considered applicable to ER (e.g. user credentials), even when ES are not used.

5 OMRON Quality Assurance System

5.1 Quality Assurance System

The OMRON Group has established a quality management system that requires meeting the OMRON Group's own provisions in addition to the requirements of the international standard ISO 9001.

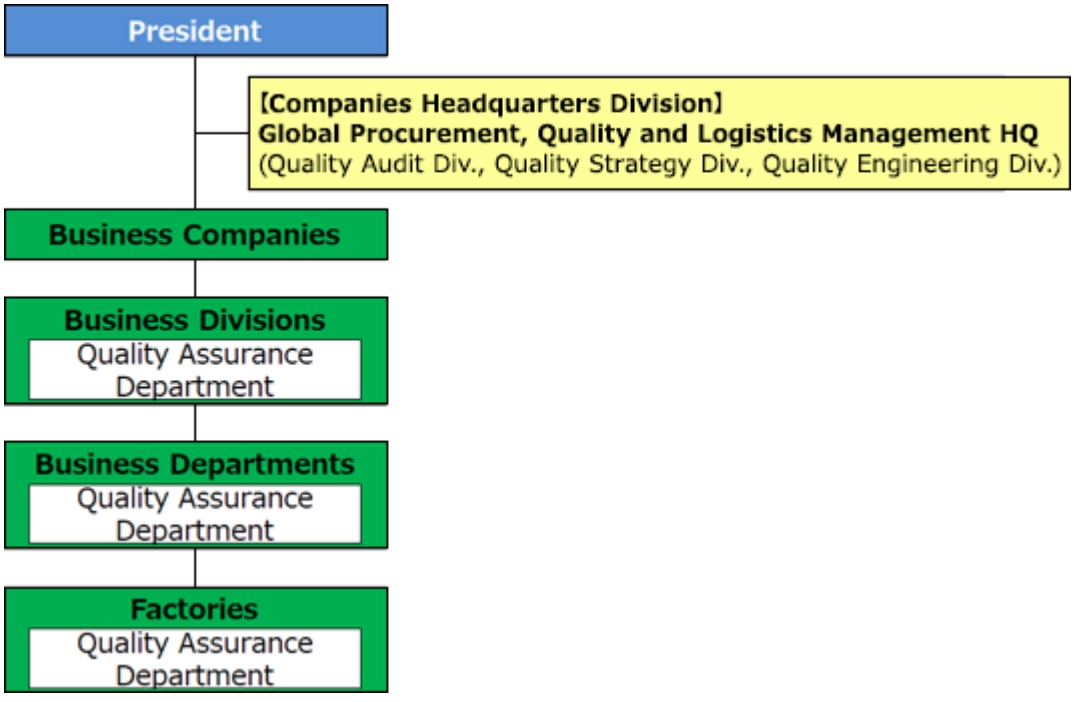
Across the OMRON Group, each organization has been strictly implementing a PDCA cycle. In this cycle, an improvement plan is formulated, the plan is implemented, and the degree of achievement is evaluated. This evaluation leads to the next improvement, and the cycle is repeated. Strict implementation of a PDCA cycle helps ensure the safety and quality of products, enabling continuous improvement of quality and prevention of quality-related problems. Concurrently, The Group has been conducting auditing to measure the efficacy of quality management systems.

As for substances that may adversely impact the environment or society, the Group has constructed a chemical substances management system in order to quickly respond to customer inquiries and provide necessary information.

The Global Procurement, Quality and Logistics Management HQ, a corporate headquarters division, has a well-established structure to support quality enhancement on a global scale, through quality approval for purchased parts and advancement of failure analysis technologies. As for purchased parts, for example, a system of evaluating and certifying suppliers' process quality is implemented to ensure the highest possible product quality throughout the world.

Also, the OMRON Group will continue its efforts to prevent silent changes* by increasing and improving the number of processed items to purchase integratedly.

* Silent change refers to changes in material composition or alteration of specifications for parts that suppliers make, without notification to clients.



OMRON Group companies clearly determine safety management systems to be implemented at each stage of its business process, from product planning and development through production, and all the way up to sales, after-sales service, and disposal. By so doing, the OMRON Group strives to ensure the supply of highly safe products.

6 References

6.1 Pharmaceutical Regulations

[1] EU Commission Directive 2003/94/EC of 8 October 2003

[2] EU Commission Directive 91/412/EEC of 23 July 1991

[3] EU GMP: EudraLex, "The rules governing medicinal products in the European Union", Volume 4 - Good Manufacturing Practice (GMP) Guidelines.

[4] EU GMP Annex 11 “Computerized Systems” (January 2011)

[5] EU GMP Annex 15 “Qualification and Validation” (October 2015).

[6] EU Guidelines on Good Distribution Practice of Medicinal Products for Human Use (24 November 2013)

[7] US Federal Food, Drug, and Cosmetic Act (FD&C Act), 1938

[8] FDA: 21 CFR Part 210 - *Current Good Manufacturing Practice in Manufacturing, Processing, Packing, or Holding of Drugs; General*

[9] FDA: 21 CFR Part 211 - *Current Good Manufacturing Practice for Finished Pharmaceuticals*

[10] FDA: 21 CFR Part 11 “Electronic Records, Electronic Signatures”, March 20, 1997

6.2 Validation Guidelines

[11] FDA: “Computerized Systems in Drug Establishments” aka the “bluebook”, February 1983.

[12] FDA: Process Validation Guidelines, 1987

[13] FDA: “General Principles of Software Validation; Final Guidance for Industry and FDA Staff”, January 11, 2002.

[14] FDA: Guidance for Industry “Part 11, Electronic Records; Electronic Signatures — Scope and Application”, August 2003

[15] ISPE: GAMP® 5 “A Risk-Based Approach to Compliant GxP Computerized Systems”. (Second Edition, July 2022)

[16] ISPE: GAMP® Good Practice Guide “A Risk-Based Approach to Electronic Records and Signatures”, February 2005

[17] ISPE: GAMP® Good Practice Guide “IT Infrastructure Control and Compliance”, September 2005

[18] ISPE: GAMP® Good Practice Guide “A Risk-Based Approach to GxP Process Control Systems” (2nd edition), February 2011

[19] ISPE: GAMP® Good Practice Guide “A Risk-Based Approach to Testing of GxP Systems” (Second Edition), December 2012.

[20] ISPE: GAMP® Good Practice Guide “Electronic Data Archiving”, July 2007

6.3 Data Integrity Guidelines

[21] PIC/S Guidance: Good Practices For Data Management And Integrity In Regulated Gmp/Gdp Environments, Documents 041-1 (final, Jul 2021)

[22] MHRA: Guideline “GMP Data Integrity Guidance and Definitions for Industry” (March 2018)

[23] WHO: Guidance On Good Data And Record Management Practices (WHO technical report series; no. 996, Annex 5 - May 2016)

[24] FDA: Data Integrity and Compliance With Drug CGMP - Questions and Answers - Guidance for Industry (final, Dec 2018)

[25] EMA: Questions and answers: Good manufacturing practice (Aug 2016)

[26] ISPE: GAMP Guide “Records and Data Integrity” (Apr 2017)

[27] ISPE: GAMP Good Practice Guide “Records and Data Integrity – Key Principles” (Nov 2018)

[28] ISPE: GAMP Good Practice Guide “Records and Data Integrity – Manufacturing Records” (May 2019)

[29] ISPE: GAMP Good Practice Guide “Records and Data Integrity – Data Integrity by Design” (Oct 2020)

6.4 Other documents

[30] ISPE: White Paper “A GAMP® Approach to Robotic Process Automation” (published in Pharmaceutical Engineering, May / June 2020)

[31] OMRON: White Paper “Automated Manufacturing in the Pharmaceutical Industry (An Introduction to the Regulations)” - Andy Avery. (2011).

[32] OMRON: White Paper “Validation of Vision Systems in the Pharmaceutical Industry (A guide to the validation of vision systems used in pharmaceutical industry using Omron components)” (2015)

[33] www: Product Safety and Quality | Product Safety and Quality | Sustainability | About OMRON | OMRON Global

[34] OMRON: Technical specifications for hardware and software components, Integration toolkit, etc.

7 Glossary

Application Program	A complete, self-contained program that performs a specific function for the user. Applications use the services of the computer operating system and other supporting applications.
AMR	Autonomous mobile robot - mobile robot that can navigate autonomously in a customer environment and does not rely on a guidance system
AMR TOP MODULE	Equipment attached to AMRs, enabling the robots to perform specific tasks based on the application requirements.
ARAM	Advanced robotics automation management
ARCL	Advanced Robotics Command Language. A simple, text-based, command-and-response operating language for AMR.
Audit Trail	An electronic or paper log used to track computer activity
Biometric	A method of verification of an individual's identity based upon measurement of the individuals' physical features or repeatable actions that are both measurable and unique to that individual.
CAPS	Cell Alignment Positioning System. A software option that uses a fixed mount target in the workspace to provide more accurate AMR positioning when approaching a destination.
CFR	Code of Federal Regulations
Closed system	An environment where system access is controlled by persons who are responsible for the content of electronic records that are on the system.
Cobot	Manipulation device (robot) designed for direct collaboration with human beings
Database	A database is a collection of data that is organized so that its contents can easily be accessed, managed, and updated.
Digital signature	An electronic signature based upon cryptographic methods or originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and integrity of the data can be verified.
Electronic records (Part 11)	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. **Part 11 Records:** • Records that are required to be maintained under predicate rule requirements and that are maintained in electronic format in place of paper format. • Records that are required to be maintained under predicate rules, that are maintained in electronic format in addition to paper format, and that are relied on to perform regulated activities. • Records submitted to FDA under predicate rules in electronic format.
Electronic signatures (Part 11)	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 handwritten signature. **Part 11 Signature:** • Electronic signatures that are intended to be the equivalent of handwritten signatures, initials, and other general signings required by predicate rules.

Encryption	The conversion of data into a form, called a cipher text, which cannot be easily understood by unauthorized people.
FDA	Food and Drug Administration.
Fleet	A group of AMRs that operate in the same area, share the same map, and are controlled by one standalone Fleet Manager or a Paired Primary Fleet Manager, operating with a Paired Secondary Fleet Manager.
Fleet Manager (Hardware)	IPC connected to the network that hosts the FLOW Core software. All fleet management capabilities of the FLOW Core software run on the Fleet Manager appliance.
Fleet Manager (Software)	The set of capabilities within the FLOW Core software that executes all fleet management activities. These include the management of maps, AMR configuration, job queue management, and traffic coordination.
Fleet Operation Workspace Core (FLOW Core)	Fleet Operations Workspace Omron's software suite that manages all autonomous mobile robot
Fleet Simulator	Configuration of the Fleet Manager in simulation mode to simulate AMR fleets.
Flow iQ	Analytics, dashboards, monitoring, historics, heatmaps…
Functionality	The sum or any aspect of what a product, such as a software application or computing device, can do for a user.
Goal	Map-defined virtual destination(s) for AMRs (e.g., pickup or drop-off points).
GxP	Incorporates GMP (good manufacturing practice), GCP (good clinical practice), GLP (good laboratory practice), GDP (good distribution practice), GVP (good vigilance practice – pharmacovigilance). NB: GDP is also used for Good Documentation Practice. GDocP is a preferred form to avoid ambiguity. GEP is used for Good Engineering Practice.
Infrastructure	The physical hardware used to interconnect computers and users. Infrastructure also includes the software used to send, receive, and manage the signals that are transmitted.
Integration Toolkit	Omron's interface application that enables integration between the Fleet Manager and the end user's client application.
Job	An AMR activity, usually consisting of either one or two "job segments". (either PICKUP or DROPOFF). The Fleet Manager receives all job requests from ARCL.
MARC Firmware	The Mobile Autonomous Robot Controller (MARC) firmware computes and reports the AMR's odometer (X. Y and heading) readings and other low-level operating conditions to ARAM.
Metadata	Data about data. In data processing, metadata is definitional data that provides information about, or documentation of other data managed within an application or environment.
MobilePLanner	The primary software application for programming AMR actions.

MobilePlanner Tablet	A limited-functionality version of the MobilePlanner software. Has tools to monitor AMRs, AMR statistics, monitor and add jobs. Does not have tools to create or edit maps.
Mobile Robot	Complete machine which consists of an OMRON AMR and minimum an AMR top module installed by the system integrator.
MoMa	Mobile Manipulator – combination of an AMR and a robot handling device, usually a cobot type OMRON TM
NJ/NX	Omron machine controller
Open system	An environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.
Operating system	The program that, after being initially loaded into the computer by a boot program, manages all the other programs in a computer.
PLC	A programmable logic controller (PLC) or programmable controller is an industrial computer that has been ruggedized and adapted for the control of manufacturing processes, such as assembly lines, machines, robotic devices, or any activity that requires high reliability, ease of programming, and process fault diagnosis.
Robot	A flexible, re-programmable machine capable of automatically executing a complex series of actions.
SetNetGo	Software OS resides on AMRs and the Fleet Manager appliance. Used to configure AMRs' communication parameters. Accessed via the SetNetGo tab in MobilePlanner.
System	The entire computer system, including input/output devices, the operating system and possibly other software
Sysmac Studio	Automation platform integrating Logic, Motion, Robotics, HMI, Vision, Sensing, Safety, and 3D Simulation
TMFlow	Operating system and configuration software of Omron TM series Cobots.
Validation	The process where software is evaluated to ensure that it complies with the requirements.
IQ	Installation Qualification
OQ	Operational Qualification
PQ	Performance Qualification. Sometimes also used to address Process Qualification (FDA)
PV	Process Validation
FAT	Factory Acceptance Test
SAT	Site Acceptance Test

First Edition, September 2023

Lead author: Sandro De Caris, further authors Wilfried Kappel, Peter Lange, Arndt Neues