Implementation of

21 CFR Part 11

Allen-Bradley · Rockwell Software

Rockwell Automation

PharmaSuite 8.4

How PharmaSuite® is helping regulated companies
to achieve compliance with 21 CFR Part 11.

This document has been approved electronically via Rockwell's Document Management System.
This document contains information which is confidential and proprietary.

DIR: 10003305443/PUB

Revision: 1.0

Period of Validity

This document is valid for the release on the cover page – PharmaSuite 8.4.

CONTENTS

Introduction

PharmaSuite …

PharmaSuite® is a suite of software applications that is tailored to the needs of the Pharmaceutical and Biotech manufacturing industry. Special regulations are in place for these industries, and many of them also apply to software that is used during the course of production of a drug product. Therefore, the software has to be developed under consideration of the pertinent regulations and related requirements. In addition, appropriate validation of the deployed software system has to be performed before it can be used in the production environment.

PharmaSuite is developed under consideration of all pertinent regulations that are relevant for its use in the Pharmaceutical and Biotech industry. This is particularly true for the features of the software itself, but also for the process how the software is developed, which is based on a mature Quality Management System. Moreover, PharmaSuite includes extensive technical, functional, and quality documentation. With that, PharmaSuite meets all pre-requisites required for a successful deployment and validation at customer's site.

… and 21 CFR Part 11

The 21 CFR Part 11 rule on electronic records and electronic signatures became effective in August of 1997. Since then, there has been an ongoing discussion in the regulated industry and its suppliers about the correct interpretation and implementation of the resulting requirements. While the general implications are clear today, there is still some need for clarification of the detailed implementation. The FDA supports this process by providing a set of forthcoming guidance documents, e.g. on terminology, validation, audit trail, and archiving issues.

Rockwell Automation actively contributes to the ongoing discussion and keeps an active dialog with both, the FDA and its customers. Strongly committed to GxP compliance of its products and services, Rockwell Automation thereby keeps track of any evolving new requirements and interpretations. New insights are fed back to product development in an immediate and continuous manner.

Purpose

The purpose of this document is to demonstrate compliance of Rockwell Automation's PharmaSuite solution with 21 CFR Part 11 as far as technical and functional requirements are affected. The most important features of the current version of PharmaSuite related to the rule are briefly described, enhanced by examples where appropriate. The Part 11 paragraphs related to the respective features are listed at the end of each section. To provide a quick overview, an index of the mentioned paragraphs is included at the end of this document.

Validation & Qualification

Validation is mandatory for every system related to 21 CFR Part 11. The validation has to be accomplished during system integration. Rockwell Automation provides comprehensive computer system validation services that comprise the appropriate validation documentation templates, active validation support in every step of a validation project, as well as competent validation consultancy.

PharmaSuite is prepared to be validated, i.e. it has successfully passed all qualification steps that can be performed independently from its final application. Final validation in the production environment may include additional configuration and extension as well as installation, operational, and performance verification. If needed, e.g. for a Dispense solution, hardware installation verification should include devices like scales and printers.

The product, delivered by Rockwell Automation, has a standard set of functionality that is accompanied by a complete set of documentation, including a functional description and qualification documentation.

Additional validation services are provided by Rockwell Automation for any validation activities performed in the course of the customer-specific integration of the system.

Ref.: §11.10(a), §11.10(h)

Version-controlled System Documentation

The user of a system that is related to 21 CFR Part 11 must apply controls to manage the system documentation. These controls shall ensure appropriate distribution of, access to, and use of documentation for system operation and maintenance. Moreover, revision and change control procedures shall exist to maintain an audit trail that documents time-sequenced development and modification of the system documentation.

Although this needs to be achieved mainly through operational means, Rockwell Automation supports this requirement by providing appropriate version-controlled system documentation and system logbooks including a document number and an associated version number that identifies each document.

Ref.: §11.10(k)

Reporting of Electronic Records

Every electronic record in PharmaSuite can be represented in human-readable and/or electronic form.

PharmaSuite allows users to create reports with standard or custom templates.

Reports may be viewed on-screen and then printed or they may be saved in the Portable Document Format (PDF, PDF/A) and then printed and stored. This is achieved by an appropriate configuration of the system.

For all reports, PharmaSuite attaches the date and time of the report printing to the report itself. Additionally, for some reports PharmaSuite will track the number of times a specific report has been generated and places the report print number on the report itself. For example, if the report has been generated five times, the system will state "Printout 5" in the report. The system also tracks and prints identification data of the user who generated the report.

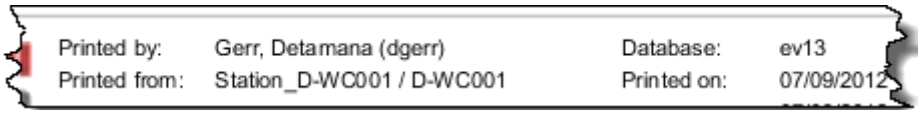


Figure 1: Report prints the database and user name (incl. login name) of the logged-in user in the footer

Figure 2: Report prints reprint information in the footer

Figure 3: Report prints the date and time of (re-)printing in the footer

Ref.: §11.10(b)

For the Batch Production Report, the Device History Report, the Workflow Report, the Master Recipe Report – Batch, the Master Recipe Report – Device, and the Master Workflow Report, the number of printouts is not being tracked, but every printout reflects the current status of the respective report with all its data at the time of printing.

Therefore, Batch Production Reports, Device History Reports, Workflow Reports, Master Recipe Reports – Batch, Master Recipe Reports – Device, and Master Workflow Reports cannot be *re*printed, but can be printed any time. As reprinting is not supported, the user who generated the report is not being tracked for these reports.

Ref.: §11.10(b)

User Authorization

The first layer of authorization in PharmaSuite is the user login. A user must have a valid login name and password to access a PharmaSuite application client.

Once logged on to PharmaSuite, the application controls user actions by associating user groups to access privileges and users to user groups. A system administrator or another authorized user assigns user groups to access privileges and users to user groups. Thus, users will inherit the privileges of the groups they are assigned to. When a user logs on to PharmaSuite, he or she will be able to perform only the actions defined in the system. By default, new users or user groups have no privileges in PharmaSuite. The system administrator or another authorized user must explicitly grant those privileges to the user or user group.

PharmaSuite contains a set of pre-configured access privileges. These privileges may be granted, in whole or in part, to users or user groups. In addition, it is possible for authorized users to define additional privileges in the system. These new privileges may then also be granted to a user or user group.

When a user is working in PharmaSuite, he or she may see tasks or menu buttons that are grayed out or not available at all without appropriate privileges. These tasks or menu buttons are not available because the user has not been given the access privileges to use these tasks or buttons. In this way, the user knows in advance that he or she does not have permission to perform an action.

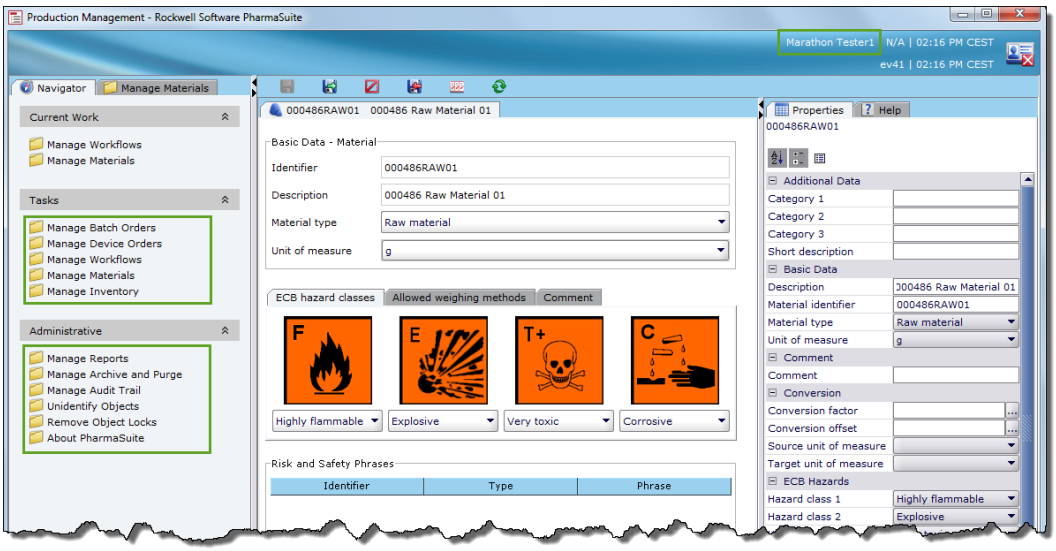


Figure 4: PharmaSuite Production Management Client (PMC) with full access privileges – 11 tasks are available in this example

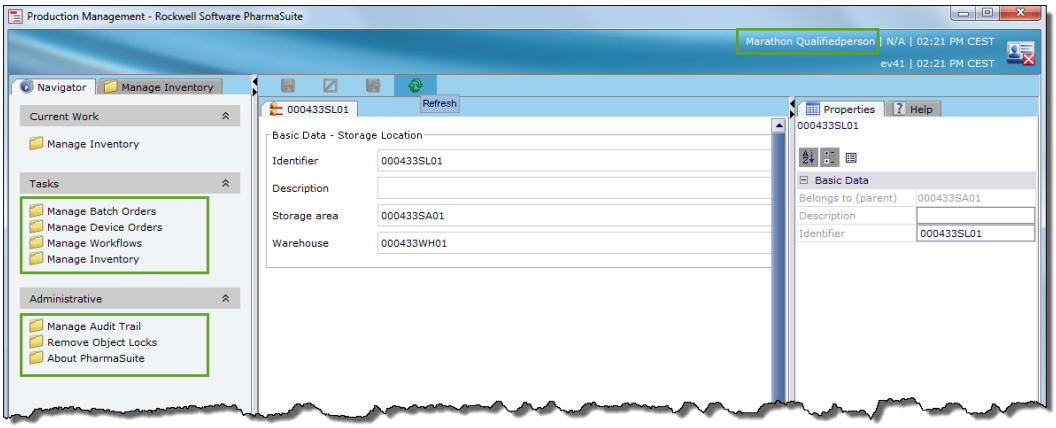


Figure 5: PharmaSuite Production Management Client (PMC) with limited access privileges – only 7 tasks are available in this example

PharmaSuite adds another component to limiting system access to authorized individuals by allowing for "certifying authorization". In this case, the system may be set up in such a way that a supervisor or another authorized user must approve that action with login name and password, and the approval is recorded as an electronic signature and linked to the record.

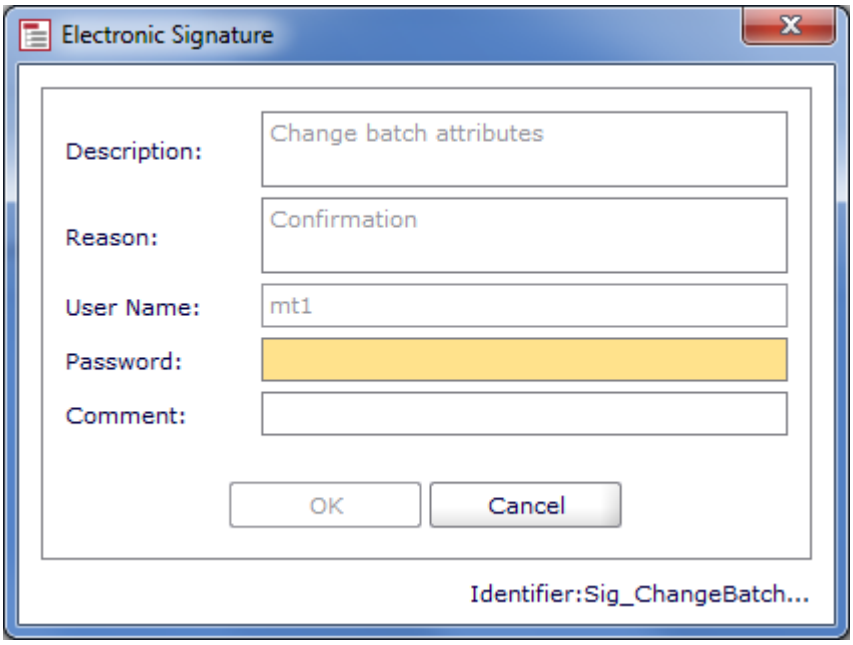


Figure 6: Electronic Signature example: Changing a batch's attributes

Ref.: §11.10(c), §11.10(d), §11.10(g)

Access Restrictions

PharmaSuite employs stringent controls to maintain the integrity of user names and passwords.

PharmaSuite ensures that each system user is uniquely identified in the system. Also, uniqueness of login names is assured – if a user needs to be removed, the account will still be maintained in the system.

PharmaSuite allows system administrators to configure how many incorrect login attempts are acceptable. Due to security aspects, the error message appearing at a wrong login attempt contains a standard text and does not contain a detailed description of the reason of failure. Once the user has exceeded the threshold for incorrect attempts, his or her account will be locked. At this point, the system administrator or another authorized user receives a notification to reset the user account.

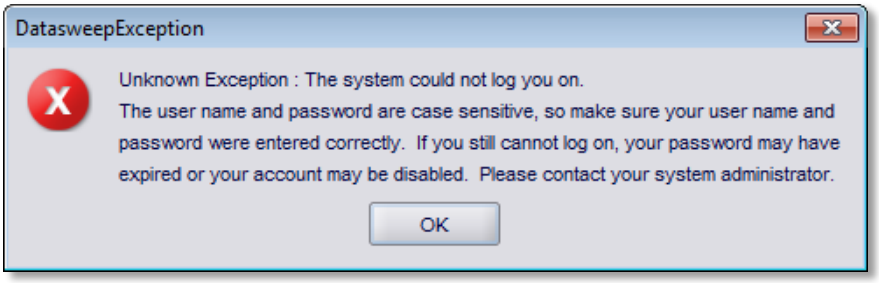


Figure 7: General error message at wrong login attempt

PharmaSuite tracks all successful logins and failed login attempts. The system prevents all users from changing any of this data.

Rigid password maintenance represents a key component in the effort to protect PharmaSuite and the operations of an enterprise. With FactoryTalk ProductionCentre Administrator (delivered with FactoryTalk ProductionCentre), you can set the Minimum Password Length, the Minimum Special Character Length, and other password security-related parameters. User passwords used for login and electronic signatures are encrypted in PharmaSuite. Although the system administrator may reset a user password, he or she is not able to see the user's existing password. The system administrator may define the expiration date of user passwords.

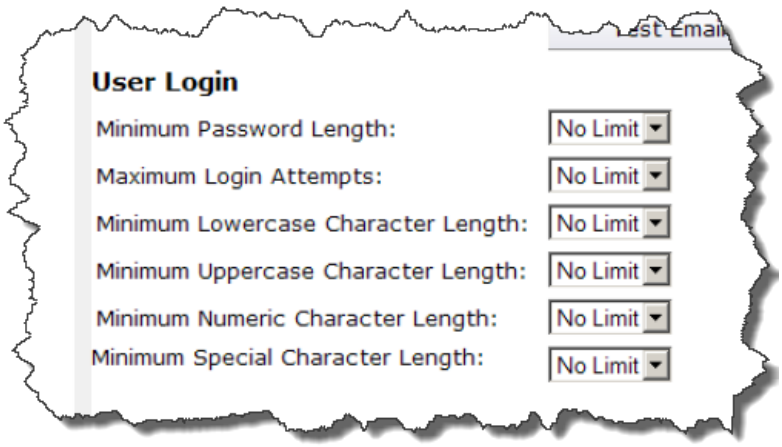


Figure 8: Security settings in FTPC Administrator

After a defined period of inactivity, PharmaSuite will use the operating system configurations to lock. This prevents unauthorized users from operating under another user's account. The system administrator may configure the duration of system inactivity that triggers the system lock. To get back into the system, after the system has been locked, the user simply has to enter his or her password.

Ref.: §11.10(c), §11.10(d), §11.10(g)

Audit Trail

PharmaSuite offers powerful functionality to manage secure, computer-generated, time-stamped audit trails associated with records and transactions.

PharmaSuite keeps various audit trail formats that track transactions of GxP-relevant master data and other data in the system. These formats range from “raw” data to logbooks and histories to status and transaction logs. An enterprise may perform a documented analysis of required audit trail data. During PharmaSuite installation, the system will be set up to capture the key audit trail data.

Audit trail-related information may be visualized in several ways in the **Production Management Client** of PharmaSuite:

- By displaying audit trail data for a number of basic master data objects, e.g. material (optional / configurable)
- By displaying the transaction history data of inventory-related objects like batches, sublots, and devices

For convenience, the recorded data of objects under audit trail can either be accessed through audit trail use cases or by using the “View audit trail for …” button (for the currently opened object). Also, the transaction history and logbook functionality is available per object.

Audit trail data cannot be deleted or altered by users; and each transaction creates a new record, so that previously recorded information will never be obscured. Audit trail records contain the following data:

- Timestamp of transaction
- Transaction type (create, delete, modify)
- Unique login name of the user who performed the transaction

Additional data is available in the database, but currently not exposed to the user by default.

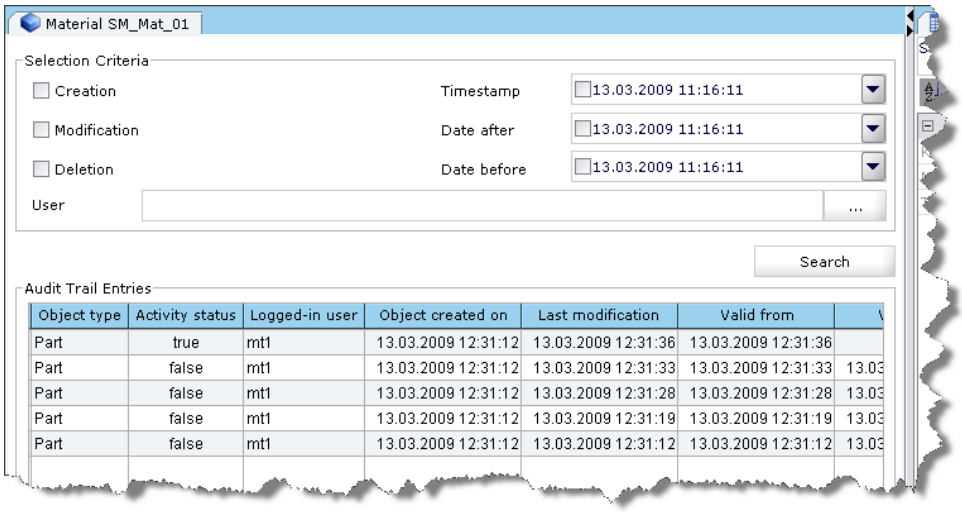


Figure 9: Modification information for a material master data object

Through the PharmaSuite version control feature of the **Recipe and Workflow Designer**, objects can be controlled by a configurable version graph that controls the process of its creation, review, approval, valid use, and archiving. Specific transitions may require an electronic signature to approve the status change (configurable).

In the default configuration, this feature is active for master recipes, workflows, and change requests. Version information can be displayed by using the “View status history” function.

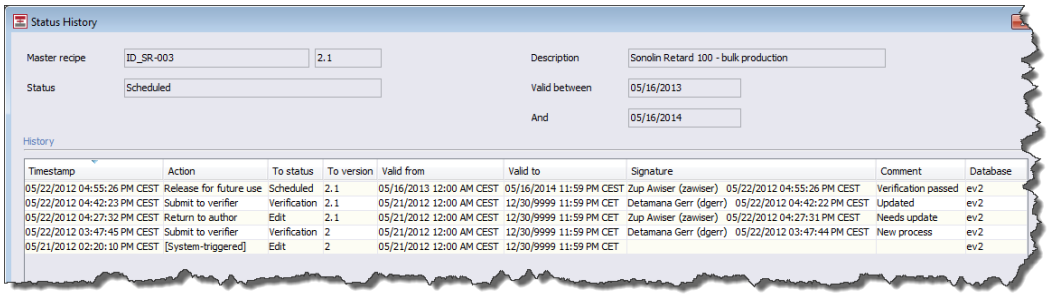


Figure 10: Status history (example)

Furthermore, the **Data Manager** provides status control for equipment classes, entities, and graphs and displays their status history. Functionality includes

- Displaying the status history of equipment classes, (template) entities, and graphs
- Displaying the change history data of equipment classes, (template) entities, and graphs
- Displaying the logbook of equipment entities
- Displaying the change history data of work centers and stations

In addition, in **Electronic Batch Recording** (EBR), data can be recorded and all changes to data that has already been committed to the database is being recorded as an exception; thereby becoming part of the batch record (and the Batch Production Report as well as the Device History Report and the Workflow Report, respectively).

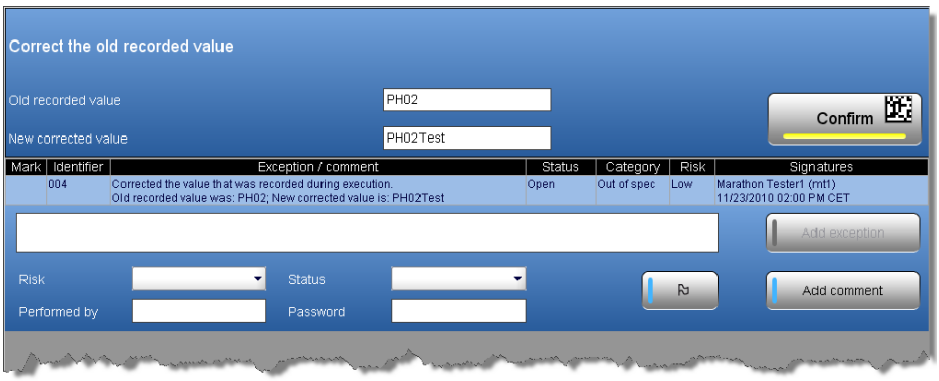
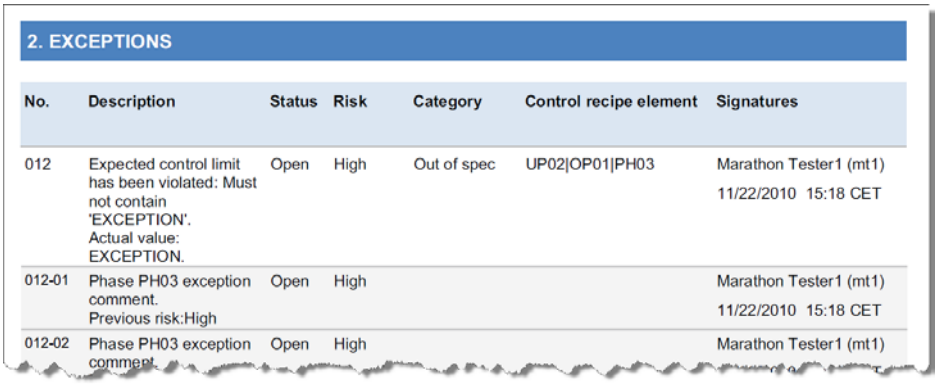


Figure 11: Correction of committed data is recorded as an exception



2. EXCEPTIONS

No.	Description	Status	Risk	Category	Control recipe element	Signatures
012	Expected control limit has been violated: Must not contain 'EXCEPTION'. Actual value: EXCEPTION.	Open	High	Out of spec	UP02|OP01|PH03	Marathon Tester1 (mt1) 11/22/2010 15:18 CET
012-01	Phase PH03 exception comment. Previous risk:High	Open	High			Marathon Tester1 (mt1) 11/22/2010 15:18 CET
012-02	Phase PH03 exception comment	Open	High			Marathon Tester1 (mt1)

Figure 12: Exceptions are printed as part of the Batch Production Report

Ref.: §11.10(e)

Sequencing of Steps & Events

A regulated production environment requires enterprises to ensure that steps and events happen in the correct order during production. PharmaSuite provides robust features to enforce this requirement.

Recipe and Workflow Designer – S88-based Master Recipes and Workflows

The strategy of PharmaSuite's Recipe and Workflow Designer is to empower recipe and workflow authors to sequence steps during recipe and workflow design. As such, step A must come before step B in production. During production based on PharmaSuite, operators may only complete steps in the order specified by the recipe and workflow author.

The S88-based recipes and workflows allow for sequential and parallel operations, forks and joins, and loops. The design of the recipe or workflow – and thereby the order of execution, i.e. the sequencing of steps – is under full control of the recipe and workflow author.

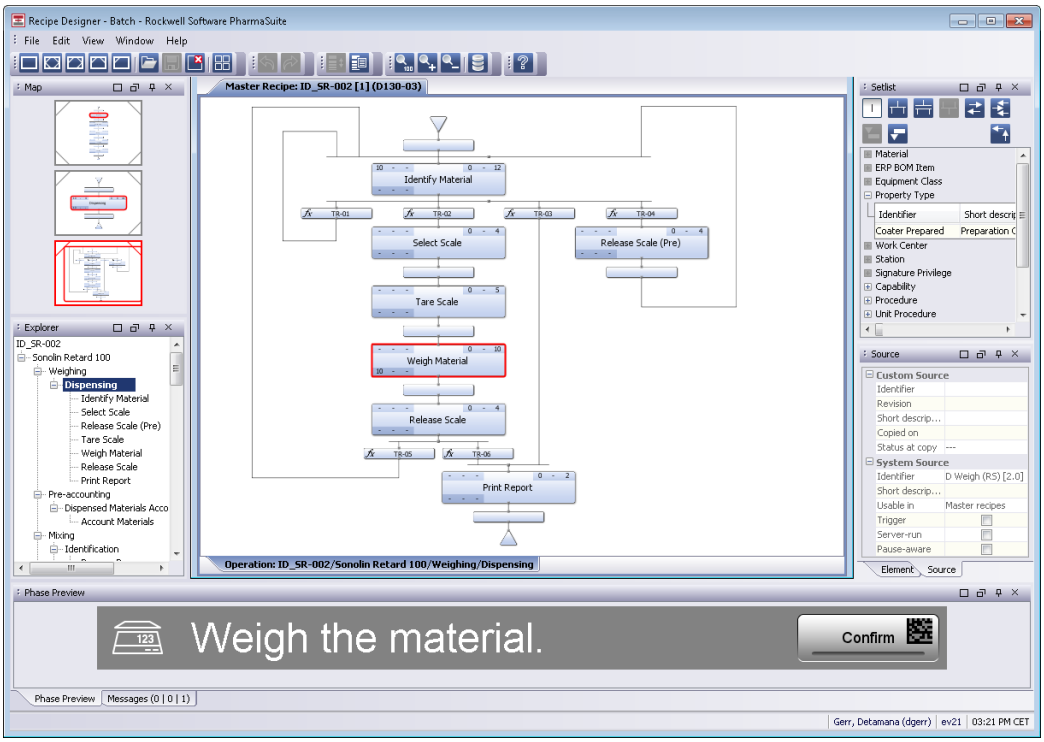


Figure 13: Recipe and Workflow Designer – a graphical workbench

In addition to providing control of the sequencing of steps, PharmaSuite also enforces the flow of material through production. It is possible to define ingoing and outgoing material flow for master recipes.

Like the sequencing of steps during the execution of a recipe or workflow, PharmaSuite also provides control over the creation of the recipe or workflow. PharmaSuite ties object statuses to approval flows. PharmaSuite gives an enterprise the power to define the transition of a recipe or workflow object from inception to validity. Each transition requires user authorization and, if required, an electronic signature.

For example, a recipe author may create a recipe for manufacturing product A. PharmaSuite prevents that recipe from being used until that object (the recipe) has reached the status “Valid”. To create valid production orders in PharmaSuite, all objects referenced in that request must be in the “Valid” status.

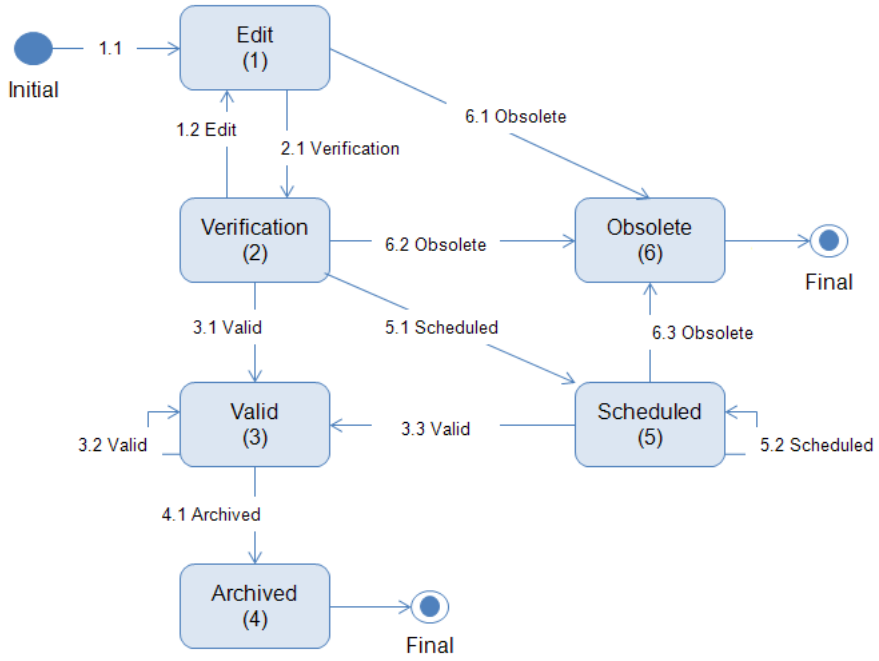


Figure 14: Default version graph for master recipes

Production Execution Client – Electronic Batch Recording

Sequencing of steps and events is enforced through the underlying SFC engine (Sequential Flow Chart) of FactoryTalk ProductionCentre by applying a set of rules to the S88-based operations as specified by the recipe and workflow author (for more information, see *Recipe and Workflow Designer – S88-based Master Recipes and Workflows*). During execution of the S88-based recipes or workflows, transitions are evaluated to trigger the phases that are being available for the operator. The sequencing logic, i.e. phases and transitions (that may depend on the data entered in previous steps), is an integral part of the recipe or workflow, and as such under full control of the recipe and workflow author.

Production Execution Client – Pre-defined Workflows

In addition, sequencing of steps and events during production execution is enforced by pre-defined (inventory) workflows. These workflows (Material Receipt, Material Issue, Relocation, Sublot Split, and Inventory Correction) are following pre-defined activities and transactions.

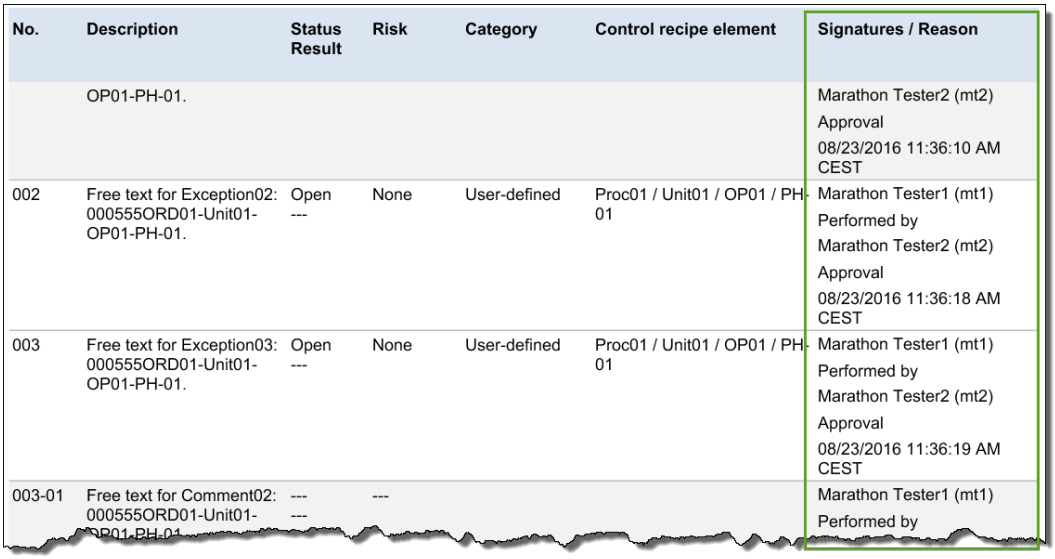
For example, in the pre-defined *Relocation* workflow, the operator needs to select one or more sublots first, then select a target location for the selected sublot(s). Finally, the relocation can be executed.

Ref.: §11.10(f)

Electronic Signature Manifestation

Electronic signatures in PharmaSuite are represented as the user's full name. The date and time of signing always appear next to each occurrence of a signature. In case of double signatures (to be used when a witness is needed), both signatures are displayed individually, but marked as belonging to the same event. Additionally, signatures can carry a defined meaning. This can be configured for each signature separately. Therefore, the user executing an electronic signature in PharmaSuite understands the meaning of what he or she is signing (see Figure 6). In PharmaSuite's Production Execution Clients, signatures are provided during processing. Hence, users understand the significance of their signature at every single step, as the signature is requested for a specific context.

All signature components are currently displayed on paper records only (e.g. Batch Production Report, Device History Report, Workflow Report), but the detailed information like name of the signer, date and time when the signature was executed, and meaning are available and stored in the database.



No.	Description	Status Result	Risk	Category	Control recipe element	Signatures / Reason
	OP01-PH-01.					Marathon Tester2 (mt2) Approval 08/23/2016 11:36:10 AM CEST
002	Free text for Exception02: 000555ORD01-Unit01-OP01-PH-01.	Open ---	None	User-defined	Proc01 / Unit01 / OP01 / PH-01	Marathon Tester1 (mt1) Performed by Marathon Tester2 (mt2) Approval 08/23/2016 11:36:18 AM CEST
003	Free text for Exception03: 000555ORD01-Unit01-OP01-PH-01.	Open ---	None	User-defined	Proc01 / Unit01 / OP01 / PH-01	Marathon Tester1 (mt1) Performed by Marathon Tester2 (mt2) Approval 08/23/2016 11:36:19 AM CEST
003-01	Free text for Comment02: 000555ORD01-Unit01-	--- ---	---			Marathon Tester1 (mt1) Performed by

Figure 15: Section of a Batch Production Report, showing electronic signatures

Ref.: §11.50(a), §11.50(b)

Signature/Record Linking

It is important for electronic signatures to be completely tied to the object that was signed. The PharmaSuite database architecture provides a secure structure to protect the signature/object relationship. PharmaSuite relies on a relational database to store this vital data. PharmaSuite users do not have access to this database, thus making the signature/object history very secure.

Handwritten signatures applied to printouts of electronic records may not be falsified since every printout is unique and is logged in the system (see also section *Reporting of Electronic Records*).

Ref.: §11.70

Electronic Signature Components and Controls

Part 11 requires that each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else. PharmaSuite meets these requirements by refusing to insert non-unique user identification codes. Moreover, user accounts in PharmaSuite that are no longer needed cannot be deleted from the database once they have been used, thereby supporting uniqueness over time.

If electronic signatures are not biometric identification, they must contain at least two distinct identification codes, such as user name and password. As discussed earlier, PharmaSuite employs effective user name/password controls.

In addition to these “logical keys”, PharmaSuite optionally provides functionality to require users to use a “physical key”. A “physical key” may be, for example, a “smart card”. Typically, the smart card would have an associated password. In some PharmaSuite production environments, enterprises utilize this rigid signature protection, with each user providing his or her user name and password as well as a smart card with its associated password. The use of a physical key is not part of the standard package, but available for projects by configuration.

The Part 11 ruling allows for using a single signature component in a sequence of signings if all signature components were executed for the first signature. If a physical token is used (e.g. smart card), the token has to be introduced once at the beginning of a series of signings. From that point on, the identification code defaults to the current user. The user name is displayed on-screen. The user has to key in his password.

Under which conditions a signature may start a series of signings depends on the current context of the signature and can be configured within PharmaSuite.

An enterprise must protect the signature data that is used to approve transactions or records. PharmaSuite helps an enterprise do so. Many of these controls are described above in section *Access Restrictions*. In addition to these controls, PharmaSuite encrypts password information in the system so that no users can see password data. Also, the password is not displayed when a user enters it into the system.

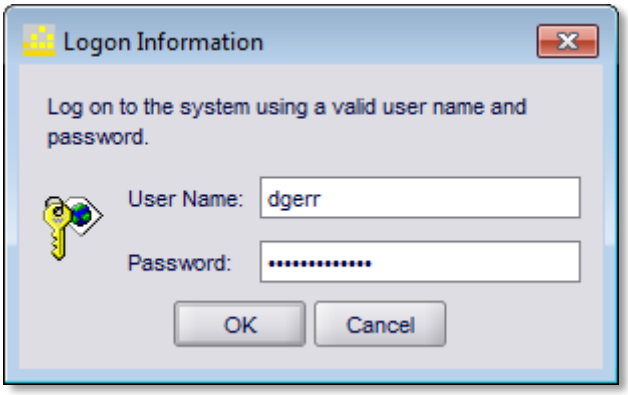


Figure 16: System logon form with masked password

Periodic revision of assigned access privileges, as required by the rule, is supported by appropriate reporting functions for user/user group data. These reporting functions display the privileges of each user and its correspondence to user groups.

PharmaSuite provides transaction safeguards to prevent unauthorized use of passwords and/or identification codes. Related to login features, these are:

- Configurable number of false login attempts
- Log of all login attempts

Moreover, if the number of false login attempts is exceeded, the user account is locked and may only be reset by the system administrator (a user with a locked account is also not permitted to provide electronic signatures).

Ref.: §11.100(a), §11.200(a)(1), §11.300 (a), §11.300 (b), §11.300 (d)

Index

Compliance to 21 CFR Part 11 paragraphs §11.10(i), §11.10(j), §11.100(b), §11.100(c), §11.200(a)(2), §11.200(a)(3), §11.200(b), §11.300(c), and §11.300(e) needs to be achieved through operational means.

Archiving, backup, and disaster recovery which help to achieve compliance with paragraph §11.10(c) are not part of PharmaSuite, but need to be achieved through operational means.

21 CFR Part 11 paragraph §11.30 does not apply to PharmaSuite.

Approvals

Approvals are captured electronically on the organization's Document Management System. The required approvers of this document include the following:

Name	Role
Martin Dittmer	Product Manager
Martin Irmisch	Test Manager
Steffen Landes	Development Manager

Appendix A: Requirements Mapping

This appendix provides a mapping of the compliance requirements specified for PharmaSuite 8.4 to the chapters of this document, based on paragraphs of 21 CFR Part 11.

Validation & Qualification (§11.10(a); §11.10(h))

SR1075.1.1	General prerequisites and usage of B2MML
SR1075.1.1.1	Prerequisites for import [Usage of B2MML]
SR1075.1.1.2	Checksum [Usage of B2MML]
SR1075.1.1.3	Handling of status and version [Usage of B2MML]
SR1075.1.1.4	Handling of status transition history [Usage of B2MML]
SR1076.16	Status graph for the QC status of batches
SR1076.16.1	Statuses for the QC Status of batches
SR1076.16.2	Default transitions for the QC Status of batches
SR1076.16.3	Additional transitions for the QC Status of batches
SR3146.2.2	Risk and safety phrases
SR3146.2.2.1	Attributes [for Risk and safety phrases]
SR3146.6	Configurable version control

Version-controlled System Documentation (§11.10(k))

None / Empty (This paragraph cannot be fulfilled by compliance requirements, but rather by the document management applied to PharmaSuite).

Reporting of Electronic Records (§11.10(b))

In addition to the requirements listed here, all exceptions of phase building blocks – specified per SR**0**???.**3**.**2**.* (more than 100 requirements) – have been intentionally left out here to enhance the reading experience. Of course, when these exceptions occur during execution, they become part of the batch record / report.

SR0050.3.1.1	Identify manually [Identify material]
SR0050.3.1.2	Undo identification [Identify material]
SR0050.3.1.3	Multiple exceptions [Identify material]

SR0300.2.3	Identify equipment entity [Identify equipment]
SR0300.2.4	Bind identified equipment Entity [Identify equipment]
SR0300.3.1.2	Undo identification [Identify equipment]
SR0300.3.1.2.1	Undo identification - Logic [Identify equipment]
SR0300.3.2.1.1	Property value check - Logic [Identify equipment]
SR0320.2.1	Unbind equipment entity [Unbind equipment]
SR1076.3.11	Batch attributes
SR1076.5.3	Status management of devices
SR1079.1.1	User-defined exceptions
SR1079.1.1.1	User-defined exceptions in Production Response Client
SR1079.1.2	User-triggered exceptions
SR1079.1.2.1	Explicit capability-related exceptions
SR1079.1.3	Post-completion exceptions
SR1079.1.4	System-triggered exceptions
SR1079.1.4.2	Implicit capability-related exceptions
SR1079.2.3	Comments related to an exception
SR1079.2.3.4	Mandatory comments in Production Execution Client
SR1084.3	Cancel order [Batch order]
SR1084.4	Status management of orders and workflows
SR1084.4.1.1	Automatic review of an order
SR1084.4.1.2	Automatic review of a workflow
SR1084.30	Change history of order definitions
SR1084.34.1	Append workflows - Related exceptions
SR1084.35.1	Reactivate non-Dispense order step - Related exceptions
SR1084.36.1	Abort non-Dispense order step - Related exceptions
SR1084.40	Export order for archive
SR1084.100.7	Cancel order [Device order]
SR1084.100.11	Export order for archive
SR1084.101.2	Append workflows
SR1084.101.2.1	Append workflows - Related exceptions
SR1084.101.3	Reactivate device order step manually
SR1084.101.3.1	Reactivate device order step - Related exceptions
SR1084.101.4	Abort device order step

SR1084.101.4.1	Abort device order step - Related exceptions
SR1085.2.10	Export workflow for archive
SR1090.4.7	Dispensing report
SR1090.4.7.5	Signature data [Dispensing report]
SR1090.4.7.6	Exceptions [Dispensing report]
SR1090.6	Reprint labels and reports
SR1095.50.1	Audit trail
SR1095.50.2.1.1	Comments [Electronic signatures]
SR1095.50.2.2	Configuring electronic signatures
SR1095.50.2.3	Performing electronic signatures
SR1095.50.2.4	Data of an electronic signature
SR1095.50.3.4.4	Viewing access privileges of users or user groups
SR1095.50.3.4.5	Viewing users or user groups of access privileges
SR1095.50.3.5.2	Password must not be displayed [Password security]
SR1099.3.10.1	Print equipment entity logbook report
SR1099.3.10.5.2	Equipment entity logbook report - Equipment entity logbook
SR3071.8.4.2.3	Import [Data Manager - Export/Import]
SR3146.11.4.3	MR report - Approval record [Master recipe report – Batch]
SR3146.13.4.3	MWF report - Approval record [Master workflow report]
SR3146.14.4.3	MR report - Approval record [Master recipe report – Device]
SR3200.2.1	Batch Production Report GUI
SR3200.2.1.1	Content [Batch production report]
SR3200.2.1.4	List of recorded exceptions [Batch production report]
SR3200.4.1.1	Content [Workflow report]
SR3200.4.1.2	List of recorded exceptions [Workflow report]
SR3200.5.1.1	Content [Device history report]
SR3200.5.1.3	List of recorded exceptions [Device history report]

User Authorization (§11.10(c); §11.10(d); §11.10(g))

SR1076.3.11	Batch attributes
SR1076.5.3	Status management of devices
SR1076.10*	Sublot operations - Inventory operations
SR1076.10.1*	Sublot operations - Quantity correction

SR1076.16	Status graph for the QC status of batches
SR1076.16.1	Statuses for the QC status of batches
SR1076.16.2	Default transitions for the QC status of batches
SR1076.16.3	Additional transitions for the QC status of batches
SR1079.1.2	User-triggered exceptions
SR1079.1.2.1	Explicit capability-related exceptions
SR1079.1.3	Post-completion exceptions
SR1079.2.1	Signatures for exceptions and comments
SR1079.2.1.1	Signatures for user-defined exceptions
SR1079.2.1.2	Signatures for exception-related comments
SR1079.2.1.3	Signatures for phase-defined exceptions
SR1079.2.1.4	Signatures for explicit capability-related exceptions
SR1079.2.1.5	Password performance
SR1079.2.3	Comments related to an exception
SR1079.2.3.4	Mandatory comments in Production Execution Client
SR1084.3.1	Cancel order - Constraints [Batch order]
SR1084.4	Status management of orders and workflows
SR1084.24	Dispatch order steps
SR1084.24.1	Dispatch Order steps manually
SR1084.24.2	Dispatch order steps – Constraints
SR1084.26.5	Access control [Batch order – Replacement item]
SR1084.27	Alternative material [Order step input – Batch order]
SR1084.28	Increase quantity of order step input [Batch order]
SR1084.29	Supplementary item [New additional item – Batch order]
SR1084.32	Reactivate aborted order step input [Batch order]
SR1084.34	Append workflows
SR1084.35	Reactivate non-Dispense order step manually
SR1084.36	Abort non-Dispense order step
SR1084.100.7.1	Cancel order - Constraints [Device order]
SR1084.101.1	Dispatch order steps
SR1084.101.1.1	Dispatch order steps manually
SR1084.101.1.2	Dispatch order steps - Constraints
SR1085.2.1	Cancel workflow

SR1085.2.1.1	Cancel workflow - Constraints
SR1085.4.1	Dispatch workflow steps
SR1085.4.1.1	Dispatch workflow steps manually
SR1085.4.1.2	Dispatch workflow steps - Constraints
SR1089.4.2	Authorization
SR1089.4.3	Dynamic behavior
SR1089.4.4	Password performance
SR1090.6.6	Electronic signature for reprint
SR1094.11	Status management of order steps and workflow steps
SR1095.50.2.1	Single and double electronic signatures
SR1095.50.2.2	Configuring electronic signatures
SR1095.50.2.3	Performing electronic signatures
SR1095.50.3.1	Authentication for system login and electronic signature
SR1095.50.3.1.1	Verification during authentication
SR1095.50.3.1.2	Invalid authentication attempt
SR1095.50.3.1.3	Logging unsuccessful authentication attempts
SR1095.50.3.1.4	Number of invalid authentication attempts exceeded
SR1095.50.3.1.5	Multiple logins per user
SR1095.50.3.1.6	Viewing system access history
SR1095.50.3.2	Management of users
SR1095.50.3.2.3	Unique login name
SR1095.50.3.2.4	Immutable login name
SR1095.50.3.2.5	Validity timeframe [User account]
SR1095.50.3.2.6	Activity status [User account]
SR1095.50.3.2.7	Number of invalid authentication attempts
SR1095.50.3.2.8	Password strength
SR1095.50.3.2.9	Expiry date [Password]
SR1095.50.3.2.10	Assigning users to user groups
SR1095.50.3.3	Management of user groups
SR1095.50.3.4.2	Access privileges for pre-defined set of functions
SR1095.50.3.4.3	Pre-defined roles and profiles
SR1095.50.3.4.4	Viewing access privileges of users or user groups
SR1095.50.3.4.5	Viewing users or user groups of access privileges

SR1099.2.6.1	Default statuses for equipment classes
SR1099.2.6.2	Default transitions for equipment classes
SR1099.3.3.7	Force unbinding an equipment entity
SR1099.3.3.8	Change properties of equipment entity in read-only status
SR1099.3.3.9	Group or separate an equipment entity
SR1099.3.8.1	Default statuses for equipment entities
SR1099.3.8.2	Default transitions for equipment entities
SR1099.4.5.2	Default transitions for equipment graphs
SR1200.1.2	Access control [Server monitoring tool]
SR1200.1.3	Resuming server-run operations
SR3071.1.1	System login
SR3071.5.3	Access control [Production Response Client]
SR3071.6.2	Access control [Recipe Designer – Batch]
SR3071.7.2	Access control [Workflow Designer]
SR3071.8.1.3	Details window [Data Manager]
SR3071.8.1.3.3	Modes of details window [Data Manager]
SR3071.8.6.1	Access rights for editing
SR3071.8.6.2	Access rights for viewing
SR3071.9.2	Access control [Recipe Designer – Device]
SR3146.6	Configurable version control
SR3146.6.4.1	Standard statuses for version control
SR3146.6.4.4	Default version graph for master workflows
SR3146.6.7.3	Serial approval [Recipe and Workflow Management]
SR3146.10.1	Status handling of building blocks
SR3146.11.4.3	MR report - Approval record [Master recipe report – Batch]
SR3146.12.2.1	Scope validity check [Change requests]
SR3146.12.2.2	Master recipe-specific change requests
SR3146.12.2.3	Master workflow-specific change requests
SR3146.13.4.3	MWF report - Approval record [Master workflow report]
SR3146.14.4.3	MR report - Approval record [Master recipe report – Device]
SR3200.3.3	Details panel [Exception Dashboard]
SR3200.3.3.2	Review an order [Exception Dashboard]
SR3200.3.3.3	Review a workflow [Exception Dashboard]

* Requirements *SR1076.10 (Sublot operations - Inventory operations)* and *SR1076.10.1 (Sublot operations - Quantity correction)* are compliance-relevant, but not marked as such in the original specification document, as they originate from “PharmaSuite 8.0 - DRS Inventory Management”.

Access Restrictions (§11.10(c); §11.10(d); §11.10(g))

SR1076.5.3	Status management of devices
SR1079.2.1	Signatures for exceptions and comments
SR1079.2.1.1	Signatures for user-defined exceptions
SR1079.2.1.2	Signatures for exception-related comments
SR1079.2.1.3	Signatures for phase-defined exceptions
SR1079.2.1.4	Signatures for explicit capability-related exceptions
SR1084.4	Status management of orders and workflows
SR1084.24	Dispatch order steps
SR1084.24.1	Dispatch order steps manually
SR1084.24.2	Dispatch order steps – Constraints
SR1084.26.5	Access control [Batch order – Replacement item]
SR1084.27	Alternative material [Order step input – Batch order]
SR1084.28	Increase quantity of order step input [Batch order]
SR1084.29	Supplementary item [New additional item – Batch order]
SR1084.32	Reactivate aborted order step input [Batch order]
SR1084.34	Append workflows
SR1084.35	Reactivate non-Dispense order step manually
SR1084.36	Abort non-Dispense order step
SR1084.101.1	Dispatch order steps
SR1084.101.1.1	Dispatch order steps manually
SR1084.101.1.2	Dispatch order steps - Constraints
SR1085.4.1	Dispatch workflow steps
SR1085.4.1.1	Dispatch workflow steps manually
SR1085.4.1.2	Dispatch workflow steps - Constraints
SR1090.6.6	Electronic signature for reprint
SR1094.11	Status management of order steps and workflow steps
SR1095.50.2.1	Single and double electronic signatures
SR1095.50.2.2	Configuring electronic signatures
SR1095.50.2.3	Performing electronic signatures

SR1095.50.3.1	Authentication for system login and electronic signature
SR1095.50.3.1.1	Verification during authentication
SR1095.50.3.1.2	Invalid authentication attempt
SR1095.50.3.1.3	Logging unsuccessful authentication attempts
SR1095.50.3.1.4	Number of invalid authentication attempts exceeded
SR1095.50.3.1.5	Multiple logins per user
SR1095.50.3.1.6	Viewing system access history
SR1095.50.3.2	Management of users
SR1095.50.3.2.2	Default user account settings
SR1095.50.3.2.3	Unique login name
SR1095.50.3.2.4	Immutable login name
SR1095.50.3.2.5	Validity timeframe [User account]
SR1095.50.3.2.6	Activity status [User account]
SR1095.50.3.2.7	Number of invalid authentication attempts
SR1095.50.3.2.8	Password strength
SR1095.50.3.2.9	Expiry date [Password]
SR1095.50.3.2.10	Assigning users to user groups
SR1095.50.3.3	Management of user groups
SR1095.50.3.4.2	Access privileges for pre-defined set of functions
SR1095.50.3.4.3	Pre-defined roles and profiles
SR1095.50.3.4.4	Viewing access privileges of users or user groups
SR1095.50.3.4.5	Viewing users or user groups of access privileges
SR1099.2.6.1	Default statuses for equipment classes
SR1099.2.6.2	Default transitions for equipment classes
SR1099.3.8.1	Default statuses for equipment entities
SR1099.3.8.2	Default transitions for equipment entities
SR1099.4.5.2	Default transitions for equipment graphs
SR1200.1.2	Access control [Server monitoring tool]
SR1200.1.3	Resuming server-run operations
SR3071.1.1	System login
SR3071.4.1.4	Automatic locking
SR3071.5.3	Access control [Production Response Client]
SR3071.6.2	Access control [Recipe Designer – Batch]

SR3071.7.2	Access control [Workflow Designer]
SR3071.8.1.3	Details window [Data Manager]
SR3071.8.1.3.3	Modes of details window [Data Manager]
SR3071.8.6.1	Access rights for editing
SR3071.8.6.2	Access rights for viewing
SR3071.9.2	Access control [Recipe Designer – Device]
SR3146.6	Configurable version control
SR3146.6.4.1	Standard statuses for Version control
SR3146.6.4.4	Default version graph for master workflows
SR3146.6.7.3	Serial approval [Recipe and Workflow Management]
SR3146.10.1	Status handling of building blocks
SR3146.12.2.1	Scope validity check [Change requests]
SR3146.12.2.2	Master recipe-specific change requests
SR3146.12.2.3	Master workflow-specific change requests
SR3200.3.3	Details panel [Exception Dashboard]
SR3200.3.3.2	Review an order [Exception Dashboard]
SR3200.3.3.3	Review a workflow [Exception Dashboard]

Audit Trail (§11.10(e))

In addition to the requirements listed here, all exceptions of phase building blocks – specified per SR**0**???.**3**.**2**.* (more than 100 requirements) – have been intentionally left out here to enhance the reading experience. Of course, when these exceptions occur during execution, they become part of the batch record / report.

SR0050.3.1.1	Identify manually [Identify material]
SR0050.3.1.2	Undo identification [Identify material]
SR0050.3.1.3	Multiple exceptions [Identify material]
SR0300.2.3	Identify equipment entity [Identify equipment]
SR0300.2.4	Bind identified Equipment Entity [Identify equipment]
SR0300.3.1.2	Undo identification [Identify equipment]
SR0300.3.1.2.1	Undo identification - Logic [Identify equipment]
SR0320.2.1	Unbind equipment entity [Unbind equipment]
SR1075.1.1.4	Handling of status transition history [Usage of B2MML]
SR1076.3.11	Batch attributes
SR1076.5.3	Status management of devices

SR1076.10*	Sublot operations - Inventory operations
SR1076.10.1*	Sublot operations - Quantity correction
SR1079.1.1	User-defined exceptions
SR1079.1.1.1	User-defined exceptions in Production Response Client
SR1079.1.2	User-triggered exceptions
SR1079.1.2.1	Explicit capability-related exceptions
SR1079.1.3	Post-completion exceptions
SR1079.1.4	System-triggered exceptions
SR1079.1.4.2	Implicit capability-related exceptions
SR1079.2.3	Comments related to an exception
SR1079.2.3.4	Mandatory comments in Production Execution Client
SR1084.3	Cancel order [Batch order]
SR1084.4	Status management of orders and workflows
SR1084.4.1.1	Automatic review of an order
SR1084.4.1.2	Automatic review of a workflow
SR1084.26.6	Change history [Batch order – Replacement item]
SR1084.27.4	Change history [Order step input – Batch order]
SR1084.28.3	Change history [Increase quantity of OSI - Batch order]
SR1084.29.4	Change history [Supplementary item – Batch order]
SR1084.30	Change history of order definitions
SR1084.32.3	Change history [Reactivate aborted OSI – Batch order]
SR1084.34.1	Append workflows - Related exceptions
SR1084.35.1	Reactivate non-Dispense order step - Related exceptions
SR1084.36.1	Abort non-Dispense order step - Related exceptions
SR1084.100.7	Cancel order [Device order]
SR1084.101.2	Append workflows
SR1084.101.2.1	Append workflows - Related exceptions
SR1084.101.3	Reactivate device order step manually
SR1084.101.3.1	Reactivate device order step - Related exceptions
SR1084.101.4	Abort device order step
SR1084.101.4.1	Abort device order step - Related exceptions
SR1088.1	Archive and purge events
SR1089.3.7.1	Usage control [API equipment logbook]

SR1089.3.7.2	FSM property status change [API equipment logbook]
SR1089.3.7.3	Phase information and signature [API equipment logbook]
SR1089.3.9	API - Equipment entity logbook data retrieval
SR1090.1	Tracking the output [Labeling and reports]
SR1095.50.1	Audit trail
SR1095.50.2	Audit trail - Visibility - Localization
SR1095.50.2.1.1	Comments [Electronic signatures]
SR1095.50.3.1.6	Viewing system access history
SR1095.50.3.2.1	Audit trail [Users]
SR1095.50.3.3.1	Audit trail [User groups]
SR1095.50.3.4.1	Audit trail [Access privileges]
SR1095.50.3.4.4	Viewing access privileges of users or user groups
SR1095.50.3.4.5	Viewing users or user groups of access privileges
SR1099.2.1.8	Change history tab [Equipment classes]
SR1099.2.1.9	Status history tab [Equipment classes]
SR1099.3.1.7	Logbook tab [Equipment entities]
SR1099.3.1.8	Change history tab [Equipment entities]
SR1099.3.1.10	Status history tab [Equipment entities]
SR1099.3.3.7	Force unbinding an equipment entity
SR1099.3.3.8	Change properties of equipment entity in read-only status
SR1099.3.3.9	Force unbinding an equipment entity
SR1099.3.10.1	Print equipment entity logbook report
SR1099.3.10.5.2	Equipment entity logbook report - Equipment entity logbook
SR1099.4.1.6	Change history tab [Equipment graphs]
SR1099.4.1.7	Status history tab [Equipment graphs]
SR1100.1.1.3	Change history tab [Work centers]
SR1100.3.3.1	Cards view [Stations]
SR1100.3.1.2	Change history tab [Stations]
SR1200.1.3	Resuming server-run operations
SR3071.8.4.2.3	Import [Data Manager - Export/Import]
SR3146.1.1.5	Audit trail [Materials]
SR3146.11.4.3	MR report - Approval record [Master recipe report – Batch]
SR3146.13.4.3	MWF report - Approval record [Master workflow report]

SR3146.14.4.3	MR report - Approval Record [Master recipe report – Device]
SR3200.2.1	Batch production report GUI
SR3200.2.1.1	Content [Batch production report]
SR3200.2.1.4	List of recorded exceptions [Batch production report]
SR3200.3.3	Details panel [Exception Dashboard]
SR3200.3.3.2	Review an order [Exception Dashboard]
SR3200.3.3.3	Review a workflow [Exception Dashboard]
SR3200.4.1.1	Content [Workflow report]
SR3200.4.1.2	List of recorded exceptions [Workflow report]
SR3200.5.1.1	Content [Device history report]
SR3200.5.1.3	List of recorded exceptions [Device history report]

* Requirements *SR1076.10 (Sublot operations - Inventory operations)* and *SR1076.10.1 (Sublot operations - Quantity correction)* are compliance-relevant, but not marked as such in the original specification document, as they originate from “PharmaSuite 8.0 - DRS Inventory Management”.

Sequencing of Steps & Events (§11.10(f))

SR0050.3.1.1	Identify manually [Identify material]
SR0300.2.3	Identify equipment entity [Identify equipment]
SR0300.2.4	Bind identified equipment entity [Identify equipment]
SR0300.3.2.1.1	Property value check - Logic [Identify equipment]
SR0300.3.2.2.1	Equipment status check - Logic [Identify equipment]
SR1075.1.1	General prerequisites and usage of B2MML
SR1075.1.1.1	Prerequisites for import [Usage of B2MML]
SR1075.1.1.2	Checksum [Usage of B2MML]
SR1075.1.1.3	Handling of status and version [Usage of B2MML]
SR1076.5.3	Status management of devices
SR1076.16	Status graph for the QC status of batches
SR1076.16.1	Statuses for the QC status of batches
SR1076.16.2	Default transitions for the QC status of batches
SR1076.16.3	Additional transitions for the QC status of batches
SR1079.1.2	User-triggered exceptions
SR1079.1.2.1	Explicit capability-related exceptions
SR1079.1.3	Post-completion exceptions
SR1079.1.4	System-triggered exceptions

SR1079.1.4.2	Implicit capability-related exceptions
SR1079.2.1.5	Password performance
SR1079.2.3	Comments related to an exception
SR1079.2.3.4	Mandatory comments in Production Execution Client
SR1084.3	Cancel order [Batch order]
SR1084.3.1	Cancel order - Constraints [Batch order]
SR1084.4	Status management of orders and workflows
SR1084.4.1.1	Automatic review of an order
SR1084.4.1.2	Automatic review of a workflow
SR1084.32	Reactivate aborted order step input [Batch order]
SR1084.34	Append workflows
SR1084.35	Reactivate non-Dispense order step manually
SR1084.36	Abort non-Dispense order step
SR1084.40	Export order for archive
SR1084.41	Purge order [Batch orders]
SR1084.100.7	Cancel order [Device order]
SR1084.100.7.1	Cancel order - Constraints [Device order]
SR1084.100.11	Export order for archive [Device order]
SR1084.100.12	Purge order [Device order]
SR1085.2.1	Cancel workflow
SR1085.2.1.1	Cancel workflow - Constraints
SR1085.2.10	Export workflow for archive
SR1085.2.11	Purge workflow
SR1089.3.5.2	Status graph [API - Usage Control of equipment entities]
SR1089.3.6.1	FSM property status management [API - Status handling of FSM properties of equipment entities]
SR1089.3.7.2	FSM property status change [API equipment logbook]
SR1089.4.3	Dynamic behavior
SR1089.4.4	Password performance
SR1094.11	Status management of order steps and workflow steps
SR1095.50.2.1.1	Comments [Electronic signatures]
SR1099.2.6.1	Default statuses for equipment classes
SR1099.2.6.2	Default transitions for equipment classes
SR1099.3.3.6	Change equipment graphs status and expiry date

SR1099.3.3.7	Force unbinding an equipment entity
SR1099.3.3.9	Group or separate an equipment entity
SR1099.3.8.1	Default statuses for equipment entities
SR1099.3.8.2	Default transitions for equipment entities
SR1099.4.1.3	Status/Trigger tab [Equipment graphs]
SR1099.4.1.4	Transition tab [Equipment graphs]
SR1099.4.5.1	Default statuses for equipment graphs
SR1099.4.5.2	Default transitions for equipment graphs
SR1200.1.3	Resuming server-run operations
SR3071.1.3	System exit
SR3071.8.4.2.3	Import [Data Manager - Export/Import]
SR3071.8.4.3	Status change operations [Data Manager]
SR3146.6	Configurable version control
SR3146.6.4	Standard statuses for version control
SR3146.6.4.1	Default version graph for master recipes
SR3146.6.4.4	Default version graph for master workflows
SR3146.6.7.3	Serial approval [Recipe and Workflow Management]
SR3146.9.3.2	Master recipe - Review mode
SR3146.9.12.2	Master workflow - Review mode
SR3146.10.1	Status handling of building blocks
SR3146.12.2.1	Scope validity check [Change requests]
SR3146.12.2.2	Master recipe-specific change requests
SR3146.12.2.3	Master workflow-specific change requests
SR3200.2.1.1	Content [Batch production report]
SR3200.3.3	Details panel [Exception Dashboard]
SR3200.3.3.2	Review an order [Exception Dashboard]
SR3200.3.3.3	Review a workflow [Exception Dashboard]
SR3200.4.1.1	Content [Workflow report]
SR3200.5.1.1	Content [Device history report]

Electronic Signature Manifestation (§11.50(a); §11.50(b))

SR1079.1.1	User-defined exceptions
SR1079.1.1.1	User-defined exceptions in Production Response Client
SR1079.1.2	User-triggered exceptions
SR1079.1.2.1	Explicit capability-related exceptions
SR1079.1.3	Post-completion exceptions
SR1079.2.1	Signatures for exceptions and comments
SR1079.2.1.1	Signatures for user-defined exceptions
SR1079.2.1.2	Signatures for exception-related comments
SR1079.2.1.3	Signatures for phase-defined exceptions
SR1079.2.1.4	Signatures for explicit capability-related exceptions
SR1079.2.3	Comments related to an exception
SR1079.2.3.4	Mandatory comments in Production Execution Client
SR1089.4.1	Signature panel
SR1090.4.7.5	Signature data [Dispensing report]
SR1095.50.1	Audit trail
SR1095.50.2.1	Single and double electronic signatures
SR1095.50.2.1.1	Comments [Electronic signatures]
SR1095.50.2.2	Configuring electronic signatures
SR1095.50.2.3	Performing electronic signatures
SR1095.50.2.4	Data of an electronic signature
SR1095.50.3.1.6	Viewing system access history
SR1095.50.3.5.2	Password must not be displayed [Password security]
SR1099.2.1.9	Status history tab [Equipment classes]
SR1099.3.1.7	Logbook tab [Equipment entities]
SR1099.3.1.10	Status history tab [Equipment entities]
SR1099.3.10.1	Print equipment entity logbook report
SR1099.3.10.5.2	Equipment entity logbook report - Equipment entity logbook
SR1099.4.1.7	Status history tab [Equipment graphs]
SR3146.11.4.3	MR report - Approval record [Master recipe report – Batch]
SR3146.13.4.3	MWF report - Approval record [Master workflow report]
SR3146.14.4.3	MR report - Approval Record [Master recipe report – Device]
SR3200.2.1	Batch production report GUI

SR3200.2.1.4	List of recorded exceptions [Batch production report]
SR3200.4.1.1	Content [Workflow report]
SR3200.4.1.2	List of recorded exceptions [Workflow report]
SR3200.5.1.1	Content [Device history report]
SR3200.5.1.3	List of recorded exceptions [Device history report]

Signature/Record Linking (§11.70)

SR1079.2.1	Signatures for exceptions and comments
SR1079.2.1.1	Signatures for user-defined exceptions
SR1079.2.1.2	Signatures for exception-related comments
SR1079.2.1.3	Signatures for phase-defined exceptions
SR1079.2.1.4	Signatures for explicit capability-related exceptions
SR1095.50.2.1	Single and double electronic signatures
SR1095.50.2.1.2	Linkage to electronic record [Electronic signatures]
SR3146.11.4.3	MR report - Approval record [Master recipe report – Batch]
SR3146.13.4.3	MWF report - Approval record [Master workflow report]
SR3146.14.4.3	MR report - Approval record [Master recipe report – Device]

Electronic Signature Components and Controls (§11.100(a); §11.200(a)(1); §11.300(a); §11.300(b); §11.300(d))

SR1079.2.1	Signatures for exceptions and comments
SR1079.2.1.1	Signatures for user-defined exceptions
SR1079.2.1.2	Signatures for exception-related comments
SR1079.2.1.3	Signatures for phase-defined exceptions
SR1079.2.1.4	Signatures for explicit capability-related exceptions
SR1079.2.1.5	Password performance
SR1089.4.4	Password performance
SR1095.50.2.1	Single and double electronic signatures
SR1095.50.2.2	Configuring electronic signatures
SR1095.50.3.1.2	Invalid authentication attempt
SR1095.50.3.1.4	Number of invalid authentication attempts exceeded
SR1095.50.3.2.2	Default user account settings
SR1095.50.3.2.3	Unique login name

SR1095.50.3.5	Password security
SR1095.50.3.5.1	Password encryption [Password security]
SR1095.50.3.5.2	Password must not be displayed [Password security]
SR1095.50.3.6.1	Password change – User-initiated
SR1095.50.3.6.2	Password change – After login
SR1095.50.3.6.3	Password change – System-forced
SR3146.6.7	Flexible definition of approval details
SR3146.6.7.1	Flexibility of user groups
SR3146.9.2.4.6	Library for signature privileges
SR3146.9.5.3	Process inputs - Signature privilege
SR3146.9.5.3.1	Process inputs - Signature privilege attributes