



SIEMENS

Edition

05/2021

COMPLIANCE RESPONSE ERES

SIMATIC

SIMATIC SIPAT V5.1

Electronic Records / Electronic Signatures
[siemens.com/pharma](https://www.siemens.com/pharma)

SIMATIC

SIMATIC SIPAT V5.1 ERES Compliance Response

Product Information

Electronic Records /
Electronic Signatures (ERES)

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Table of contents

1	Introduction	5
2	The Requirements in Short	7
3	Meeting the Requirements with SIMATIC SIPAT	9
3.1	Lifecycle and Validation of Computerized Systems	9
3.2	Suppliers and Service Providers	10
3.3	Data Integrity	10
3.4	Audit Trail, Change Control Support	11
3.5	System Access, Identification Codes and Passwords	14
3.6	Electronic Signature	15
4	Evaluation List for SIMATIC SIPAT	17
4.1	Lifecycle and Validation of Computerized Systems	17
4.2	Suppliers and Service Providers	19
4.3	Data Integrity	20
4.4	Audit Trail, Change Control Support	21
4.5	System Access, Identification Codes and Passwords	22
4.6	Electronic Signature	24
4.7	Open Systems	27

Introduction

Life science industry is basing key decisions on regulated records that are increasingly generated, processed and kept electronically. Reviews and approval of such data are also being provided electronically. Thus the appropriate management of electronic records and electronic signatures has become an important topic for the life science industry.

Accordingly, regulatory bodies defined criteria under which electronic records and electronic signatures will be considered as reliable and trustworthy as paper records and handwritten signatures executed on paper. These requirements have been set forth by the US FDA in 21 CFR Part 11 (21 CFR Part 11 Electronic Records; Electronic Signatures, US FDA, 1997; in short: *Part 11*) and by the European Commission in Annex 11 of the EU GMP Guideline (EU Guidelines to Good Manufacturing Practice, Volume 4, Annex 11: Computerised Systems, European Commission, 2011; in short: *Annex 11*).

Since requirements on electronic records and electronic signatures are always tied to a computerized system being in a validated state, both regulations also include stipulations on validation and lifecycle of the computerized system.

Application of *Part 11* and *Annex 11* (or their corresponding implementation in national legislation) is mandatory for the use of electronic records and electronic signatures. However, these regulations are only valid within their defined scope.

The scope of both regulations is defined by the regional market to which the finished pharmaceutical product is distributed and by whether or not the computerized systems and electronic records are used as part of GMP-regulated activities (see Part 11.1 and Annex 11 Principle).

Supplemental to the regulations, a number of guidance documents, good practice guides and interpretations have been published in recent years to support the implementation of the regulations. Some of them are referred to within this document.

To help its clients, Siemens, as supplier of SIMATIC SIPAT, has evaluated the system with regard to these requirements and published its results in this Compliance Response. The compliance statement is issued for the standard SIMATIC SIPAT system. Different architectures may result in a different level of compliance.

SIMATIC SIPAT V5.1 fully meets the functional requirements for the use of electronic records and electronic signatures.

Operation in conformity with the regulations is ensured in conjunction with organizational measures and procedural controls to be established by the regulated user. Such measures and controls are mentioned in chapter "Evaluation List for SIMATIC SIPAT (Page 17)" of this document.

This document is divided into three parts:

1. Chapter "The Requirements in Short (Page 7)" provides a brief description of the requirement clusters.
2. Chapter "Meeting the Requirements with SIMATIC SIPAT (Page 9)" introduces the functionality of SIMATIC SIPAT as means to meet those requirements.
3. Chapter "Evaluation List for SIMATIC SIPAT (Page 17)" contains a detailed system assessment on the basis of the individual requirements of the relevant regulations.

The Requirements in Short

Annex 11 and Part 11 take into account that the risk of manipulation, misinterpretation and changes without leaving a visible trace is higher with electronic records and electronic signatures than with conventional paper records and handwritten signatures. Furthermore the means to restrict access to electronic records to authorized individuals are very different to those required to restrict access to paper records. Additional measures are required for such reasons.

The terms "electronic record" / "electronic document" mean 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.

The term "electronic signature" means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature. Since electronic signatures are also considered as being electronic records by themselves, all requirements for electronic records are applied to electronic signatures too.

The following table provides an overview of the requirements from both regulations.

Requirement	Description
Lifecycle and Validation of Computerized Systems	<p>Computerized systems used as a part of GMP-related activities must be validated. The validation process should be defined using a risk-based approach. It should cover all relevant steps of the lifecycle and must provide appropriate documented evidence.</p> <p>The system's functionality should be traceable throughout the lifecycle by being documented in specifications or a system description.</p> <p>A formal change control procedure as well as an incident management should be established. Periodic evaluation should confirm that the validated state of the system is being maintained.</p>
Suppliers and Service Providers	<p>Since competency and reliability of suppliers and service providers are considered key factors, the supplier assessment should be decided on a risk-based approach. Formal agreements should exist between the regulated user and these third parties, including clear responsibilities of the third party.</p>
Data Integrity	<p>Under the requirements of both regulations, electronic records and electronic signatures must be as reliable and trustworthy as paper records.</p> <p>The system must provide the ability to discern altered records. Built-in checks for the correct and secure handling of data should be provided for manually entered data as well as for data being electronically exchanged with other systems.</p> <p>The system's ability to generate accurate and complete copies is essential for the use of the electronic records for regulated purposes, as well as the accessibility, readability, and integrity of archived data throughout the retention period.</p>

Requirement	Description
Audit Trail, Change Control Support	<p>Besides recording changes to the system as defined in the lifecycle, both regulations require that changes on GMP-relevant data are being recorded.</p> <p>Such an audit trail should include information on the change (before / after data), the identity of the operator, a time stamp, as well as the reason for the change.</p>
System Access, Identification Codes and Passwords	<p>Access to the system must be limited to authorized individuals. Attention should be paid to password security. Changes on the configuration of user access management should be recorded.</p> <p>Periodic reviews should ensure the validity of identification codes. Procedures should exist for recalling access rights if a person leaves and for loss management.</p> <p>Special consideration should be given to the use of devices that bear or generate identification code or password information.</p>
Electronic Signature	<p>Regulations consider electronic signatures being legally binding and generally equivalent to handwritten signatures executed on paper.</p> <p>Beyond requirements on identification codes and passwords as stated above, electronic signatures must be unique to an individual. They must be linked to their respective electronic record and not be copied or otherwise being altered.</p>
Open Systems	<p>Open systems might require additional controls or measures to ensure data integrity and confidentiality.</p>

Meeting the Requirements with SIMATIC SIPAT

The Siemens recommendations for the system architecture, conception, and configuration will assist system users in achieving compliance. For additional information and assistance see SIMATIC SIPAT 5.1 User Manual.

The requirements explained in chapter "The Requirements in Short (Page 7)" can be met by applying the following types of controls on a computerized system:

- **Technological controls**
Technological controls are technical or functional features of the used software. The required technological controls cover features contained in the standard SIMATIC SIPAT software and features built in the custom software developed on top of the standard SIMATIC SIPAT software.
The standard technological controls in SIMATIC SIPAT designed to meet regulatory requirements are covered in this document. These controls are configurable to meet more specific user/regulatory requirements.
 - Implementing these technological controls is for standard features the responsibility of the supplier.
 - It is the shared responsibility of the system integrator and the customer to enforce compliancy when configuring standard technological controls.
 - It is the shared responsibility of the system integrator and the customer to enforce compliancy for the custom software.
- **Procedural controls**
Procedural controls are standard operating procedures on the use of the application software or on the environment in which the software is used.
It is the responsibility of the customer to implement the procedural controls to support regulatory compliance.
- **Administrative controls**
Administrative controls are procedures on system administration, such as system access, user management, password management, ...
It is the responsibility of the customer to implement the administrative controls to support regulatory compliance.

The requirements explained in chapter "The Requirements in Short (Page 7)" can be supported by the system as follows.

3.1 Lifecycle and Validation of Computerized Systems

In Annex 11 from 1992 and in Part 11 from 1997, the law already required that computerized systems need to be validated. Criteria for the validation of the system and its lifecycle were added in the edited revision of Annex 11 from 2011.

Nonetheless the requirements to validate a computerized system and to keep it in a validated state had long been a part of regulations other than *Part 11* and *Annex 11*. This was the motivation for the ISPE (International Society of Pharmaceutical Engineers, <http://>

3.3 Data Integrity

www.ispe.org) to publish practical guidance like the Baseline Guides (Baseline® Pharmaceutical Engineering Guides for New and Renovated Facilities, Volume 1-7, ISPE), the GAMP 5 guide (GAMP 5 – A Risk-Based Approach to Compliant GxP Computerized Systems, ISPE, 2008) as well as the GAMP Good Practice Guides.

Thus the system lifecycle as well as the approach to validation should be defined considering the guidance from the GAMP 5 guide. The guide also includes a number of appendices for lifecycle management, system development and operation of computerized systems.

Since most pharmaceutical companies already have a validation methodology for computerized systems as a part of their process landscape, it is preferable to set up the systems lifecycle and validation according to these.

3.2 Suppliers and Service Providers

Suppliers of systems, solutions and services must be evaluated accordingly, see GAMP 5 Appendix M2. Siemens as a manufacturer of hardware and software components follows internal procedures of Product Lifecycle Management and works according to a Quality Management System, which is regularly reviewed and certified by an external certification company.

3.3 Data Integrity

Data integrity is assured in the system by measures like access protection, audit trail, data type checks, checksums, backup/restore, and archiving/retrieval, completed by system validation, appropriate procedures and training for personnel.

Archiving

SIMATIC SIPAT offers the possibility to archive measurement data present in the operational central database to an archive database (short-term storage) and subsequently to a long-term archive medium such as a file server (standard SIMATIC SIPAT functionality).

Short-term archiving

The data synchronization between the operational and archive database is a continuous action without user interaction. Records stored in the archive database are accessible through the SIMATIC SIPAT Data Miner module and the SIMATIC SIPAT reports (reporting is provided as an option with the system).

If short-term archiving is implemented the SIMATIC SIPAT system is running in replicated mode. If short-term archiving is not implemented the SIMATIC SIPAT system is running in stand-alone mode.

Long-term archiving

Long-term archiving is based on using XML files. The data integrity of these XML files is secured by a checksum. When moving the data to the long-term storage, it is copied first, verified with the data in the database and only with successful verification it is deleted from the database. Such activities in the database are fully traceable and audit trailed.

Long-term archiving can run on a system in stand-alone mode (archiving data from the operational central database) or on a system in replicated mode (archiving data from the archive database). If the data is moved from the archive database and the same data is still present on the operation database, it is deleted first from the operation database to avoid inconsistencies.

The long-term archiving can run automatically: SIMATIC SIPAT automatically creates tasks which define the methods to be archived.

Archiving tasks can also be created manually: the user defines the measurement date to be archived by selecting the relevant SIMATIC SIPAT methods.

It is the regulated user's responsibility to administer the long-term archived data and to comply with the data retention period.

For more information on how to manage archiving in SIMATIC SIPAT, see the user manual of SIMATIC SIPAT 5.1.

3.4 Audit Trail, Change Control Support

"Audit trails are of particular importance in areas where operator actions generate, modify, or delete data in the course of normal operation." (Guidance for Industry Part 11 – Scope and Application, FDA, 2003)

An audit trail is not required for automatically generated electronic records which can neither be modified nor deleted by the operator. The system provides adequate system security mechanisms for such electronic records (e.g. access protection).

The following sections describe the implementation of requirements with regard to the audit trails during runtime operation and provide information on tracking changes made in the configuration module of SIMATIC SIPAT.

Audit trail functionality in SIMATIC SIPAT is provided on all runtime operation records. The audit trail records:

- are secure, computer-generated and time-stamped (date and time);
- contain the user ID and user name of the person responsible for making the change;
- are available for review.

Original record data remains accessible even when changes or deletions are made to a record. Additionally, security is provided on all records to prevent additions, modifications, or deletions outside the controlled environment.

It is the responsibility of the customer to ensure time synchronization between all used IT equipment.

Change control support is provided on all configuration records. All changes to a configuration object are recorded in the history of this object. These change records have the same properties as the audit trail of runtime records.

Audit trail

When a configuration object is activated in the runtime module, an operational object is created. An operational object is created by using the information of a specific version of the (corresponding) configuration object. Next to the various actions that can be performed on operational object (like start, stop, etc) only individual properties (like context data, manual, info data, etc.) on operational objects can be changed. These actions and changes are logged in the audit trail.

Following details are stored in the database:

- ID of the corresponding configuration object;
- Version of the corresponding configuration object;
- Local date and time;
- UTC date and time;
- User ID (Microsoft Windows account);
- User name (Microsoft Windows user name);
- Short description of the action (e. g. reason);
- Details of the action or of the changed property, including old and new value if applicable.

Data measured with a validated (GMP) method can unambiguously be linked to the configuration for all settings.

Data measured with non-GMP methods can unambiguously be linked to the configuration for most settings.

The audit trail can be exported using the standard reports of the SIMATIC SIPAT software.

Audit trail on short-term archiving actions

Operational data that is archived (see chapter "Data Integrity (Page 10)") can be deleted from the operational database when the archiving is verified. The following audit trail of the deletion action is stored in the database:

- The identification of the deleted data. For runtime methods this is the method runtime ID (ME), the method instance ID (MI) and its context;
- Who has scheduled the deletion (user name and user ID);
- Timestamp of the deletion;
- Details of the deletion.

Audit trail on long-term archiving actions

Archived data can be copied or moved to a long-term archive medium such as a file server. This action is fully audit trailed. It contains:

- The identification of the copied or moved data, which is the method runtime ID (ME), the method instance ID (MI) and its context;
- The original (XML) file location including the file name;
- Who has scheduled the archiving (user name and user ID);
- Timestamp of the archiving;
- Details of the archiving.

Change control support

Change control support is provided for:

- configuration objects
 - station definitions
 - method definitions
 - collector definitions
 - calculation definitions
 - info data sheet definitions
 - workstation definitions
- data miner objects
 - data sheets

Change control support is provided by two features: the history and the version control of an object.

Object history

The history of a configuration object is displayed in 4 columns on the "Audit Trail" tab of the object: What, When, Who and Details:

What	Explains which type of change was performed to the object: this can be a property change, a state change, etc... (short description).
When	Shows at what time and date the change was affected.
Who	Shows the user name and user ID of the person that made the change.
Details	Explains which property or state that was changed with the corresponding original and new values (detailed description).

All signings, successful or unsuccessful, of an electronic signature are recorded in the history.

The time stamp of the change is stored in both local and UTC date and time. The information about the change is read-only; users can't update nor delete.

Users have the option to add comments when applicable; this is also logged in the history.

3.5 System Access, Identification Codes and Passwords

Id	When	User Id	User Name	What	Details
4107	5/10/2017 12:39:40	SIPATICARLA	Carla Van den Meerssche	New Method created	<Id>=11754-MT-A-01' <MT>=11754-MT-A-01' <VERSION>=001.00' <DESCRIPTION>=11754-MT-A-01' <IS_CURRENT>=False' <IS_MODIFIABLE>=True' <IS_EXECUTABLE>=False' <IS_DELETABLE>=False' <SS>=ED' <USAGE_CONDITIONS>=Enter Usage Conditions' <OPERATION_CONDITIONS>=Enter Operation Conditions' <REF_SOURCE>=this method' <SYNCHRONISED>=True' <CREATION_DATE_LOCAL>=5/10/2017 12:39:40' <CREATION_DATE_UTC>=5/10/2017 10:39:40' <MEAS_RATE>=10' <MEAS_RATE_UOM>=Seconds' <DYN_TIME_ALIENMENT>=False' <TP>=MT' <D>=11754-MT-A-01' <VERSION>=001.00' <D>=Pharma+
4110	5/10/2017 12:40:58	SIPATICARLA	Carla Van den Meerssche	Property changes of [Method 11754-MT-A-01 001.00]	<ST> changed from 'empty' to 'X640ISIPATQAW10' <ST_VERSION_REF> changed from 'empty' to '2' <MT>=11754-MT-A-01' <VERSION>=001.00' <PAT_ID>=11754-SIM1-A-01.1' <CL>=11754-SIM1-A-01' <CL_VERSION>=001.00' <CL_SEQ>=0' <SYNCHRONOUS>=True' <SETTINGSET>=DEFAULT' <MEAS_RATE>=10' <MEAS_RATE_UOM>=Seconds' <CL_VERSION_REF>=2' <CL>=11754-SIM1-A-01' <CL_SEQ>=0' <CL_VERSION>=001.00' <EXPRESSION>=LastValue' <MT>=11754-MT-A-01' <NEG_VAL_RANGE>=10' <NEG_VAL_RANGE_UOM>=Seconds' <PAT_ID>=Sin' <POS_VAL_RANGE>=0' <POS_VAL_RANGE_UOM>=Seconds' <SEQUENCE>=1' <SOURCE_ID>=Sin' <VERSION>=001.00' <X_TP>=MultiValue' <PERSIST>=True' Signed electronically by Carla Van den Meerssche (SIPATICARLA) meaning: comment
4112	5/10/2017 12:41:26	SIPATICARLA	Carla Van den Meerssche	Added [Collector input Sin] to [Collector 11754-SIM1-A-01.1]	<IS_MODIFIABLE> changed from 'True' to 'False' <IS_EXECUTABLE> changed from 'False' to 'True' <SS> changed from 'ED' to 'AP' No signature required
4113	5/10/2017 12:41:37	SIPATICARLA	Carla Van den Meerssche	State Changed from [In Editing] to [Approved]	<IS_MODIFIABLE> changed from 'False' to 'True' <IS_EXECUTABLE> changed from 'True' to 'False' <SS> changed from 'AP' to 'ED' <MT>=11754-MT-A-01' <VERSION>=001.00' <SRC_MT>=11754-MT-B-01' <SRC_MT_VERSION>=001.00' <SRC_MT_VERSION_REF>=2' <MT>=11754-MT-A-01' <VERSION>=001.00' <SRC_MT>=11754-MT-B-01' <SRC_MT_VERSION>=001.00' <PAT_ID>=Sin' <MTB>=Sin' <SOURCE_ID>=Sin' <SEQUENCE>=1' <X_TP>=MultiValue' <EXPRESSION>=LastValue' <NEG_VAL_RANGE_UOM>=Seconds' <POS_VAL_RANGE_UOM>=Seconds' <NEG_VAL_RANGE>=10' <POS_VAL_RANGE>=0' <MT>=11754-MT-A-01' <VERSION>=001.00' <SRC_MT>=11754-MT-B-01' <SRC_MT_VERSION>=001.00' <PAT_ID>=Sin' <MTB>=Sin' <SOURCE_ID>=Integer' <SEQUENCE>=2' <X_TP>=SingleValue' <DATA_TP>=Double' <EXPRESSION>=LastValue' <NEG_VAL_RANGE_UOM>=Seconds' <POS_VAL_RANGE_UOM>=Seconds' <NEG_VAL_RANGE>=10' <POS_VAL_RANGE>=0' PAT Collector Input Sin_MTB Signed electronically by Carla Van den Meerssche (SIPATICARLA) meaning:
4125	5/10/2017 12:44:03	SIPATICARLA	Carla Van den Meerssche	Added [PAT Collector 11754-MT-B-01 001.00]	
4126	5/10/2017 12:44:03	SIPATICARLA	Carla Van den Meerssche	Added [PAT Collector Input Sin_MTB] to [PAT Collector 11754-MT-B-01 001.00]	
4127	5/10/2017 12:44:03	SIPATICARLA	Carla Van den Meerssche	Added [PAT Collector Input Int_MTB] to [PAT Collector 11754-MT-B-01 001.00]	
4128	5/10/2017 12:45:04	SIPATICARLA	Carla Van den Meerssche	Removed [PAT Collector Input Sin_MTB] from [PAT Collector 11754-MT-B-01 001.00]	
4134	5/10/2017 12:47:10	SIPATICARLA	Carla Van den Meerssche	State Changed from [In Editing] to [Approved]	

Figure 3-1 Object history seen from the audit trail tab

Version control

Configuration objects can be subject to change control.

This implies that changes to a configuration object:

- must be logged in the object history;
- may not obscure previously recorded information.

The former is realized as described above. The latter is implemented in SIMATIC SIPAT by means of version control.

When a user wants to change the properties of a configuration object in status “Approved”, a new version must be created. Older versions in status “Approved” can neither be altered nor deleted. The audit trail of the new object mentions the version on which the new version is based.

The exact properties of the configuration object life cycle can be modified on a project basis. If this is done, the impact of this modification on the answers in this document should be evaluated. This is the regulated user's responsibility.

Deleting electronic records at configuration level is not possible, however validated records can be recalled or made obsolete.

3.5 System Access, Identification Codes and Passwords

Users must be assigned the required access rights only, in order to prevent unauthorized access to and unintended manipulation of the file system, directory structures, and system data.

The requirements regarding access security are fully met in combination with procedural controls, such as those for "specifying the responsibility and access authorization of the system users".

There is extensive security and access control for the system. Security limits access to the different parts of the application (configuration access, operation access, administrative access and access to runtime data; as well as any subset of the listed SIPAT module access).

Access to the system and to functions within the system is based on the used Microsoft Windows user ID (Microsoft Windows authentication) for login, on the user's SIMATIC SIPAT role(s) and user's functional access rights.

SIMATIC SIPAT is delivered with a default set of functional access rights for default SIMATIC SIPAT roles. Which functional access rights are allowed for which SIMATIC SIPAT roles can be adapted on a project basis and is the responsibility of the regulated user.

Users log on to SIMATIC SIPAT with two components: user ID and password.

Both fields are empty in the logon screen. The user ID and the password are never saved in the registry or anywhere else.

All logon attempts to the application, valid and invalid, are registered. By default, the user account will be locked out after three consecutive invalid logon attempts. This login verification and lock-out strategy is in addition to any policy defined on Windows domain level.

It is the regulated user's responsibility to assure correct system access and to prevent unauthorized use of the SIMATIC SIPAT system or its databases with special care for:

- Database owner and database administrator access must be procedurally controlled.
- Users with controlled access should only be granted access to SIMATIC SIPAT via existing schemas in the SIMATIC SIPAT database (e.g. SIPAT_READ, SIPAT_WRITE, SIPAT_DATAMINER) as described in the installation manual.
- All other access permissions to the central database must be verified.

3.6 Electronic Signature

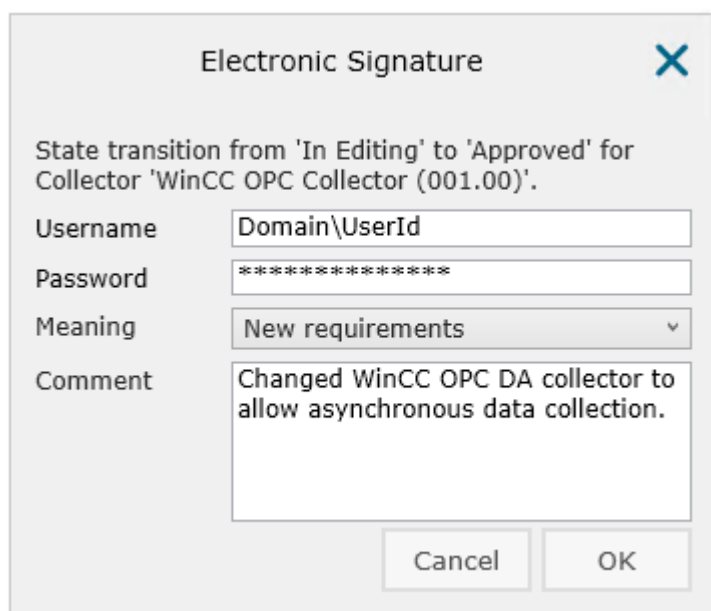
SIMATIC SIPAT provides functions for configuring an electronic signature. The variables which require an electronic signature upon changes are specified during the configuration phase of the system.

The electronic signature is being executed in a separate dialog in which the user must sign electronically by confirming the intended action with entering his user ID and password. Depending on the configuration of the electronic signature, a meaning must be selected and/or a comment must be added.

The comment can be configured as optional or mandatory for each operation. Using the default installation, comments are optional and a meaning for an electronic signature is not enabled.

Subsequently the electronic signature is saved in the audit trail along with the user ID, username, timestamp, the meaning, the comment, and the action performed.

3.6 Electronic Signature



The dialog box is titled "Electronic Signature" and contains the following fields and controls:

- Title:** State transition from 'In Editing' to 'Approved' for Collector 'WinCC OPC Collector (001.00)'.
- Username:** Domain\UserId
- Password:** *****
- Meaning:** New requirements
- Comment:** Changed WinCC OPC DA collector to allow asynchronous data collection.
- Buttons:** Cancel, OK

Figure 3-2 Electronic Signature

Evaluation List for SIMATIC SIPAT

The following list of requirements includes all regulatory requirements from 21 CFR Part 11 as well as from Annex 11 of the EU-GMP Guidelines. All requirements are structured in the same topics as those introduced in the chapter "The Requirements in Short (Page 7)" of this Compliance Response.

The *requirements* listed fully consider both regulations, regardless of whether technological or procedural controls or a combination of both are needed to fully comply with Part 11 and Annex 11.

The *answers* include, among other things, information about how the requirement is handled during the development of the product and which measures should be implemented during configuration and operation of the system. Furthermore, the answers include references to the product documentation for technical topics and to the GAMP 5 guide for procedural controls that are already considered in the guide.

4.1 Lifecycle and Validation of Computerized Systems

The fundamental requirement that a computerized system, used as a part of GMP related activities, must be validated is extended in the revision of Annex 11 from 2011 by requirements detailing expectations on a system's lifecycle.

	Requirement	Reference	Answer
4.1.1	Risk management should be applied throughout the lifecycle of the computerized system.	Annex 11, 1	Yes. The Product Lifecycle Management (PLM) process is the R&D process for Siemens software products. This process incorporates risk management accordingly. During the validation of a customer-specific application, risk management should be ensured by the regulated user.
4.1.2	Validation of a system ensures its accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	21 CFR 11.10 (a)	Yes. The development of the software product (COTS, see Annex 11, glossary) is subject to the control of the Siemens QMS and the PLM process. The regulated user should take appropriate measures to validate the application (see Annex 11, glossary), as well as maintaining its validated state.
4.1.3	Validation documentation covers relevant steps of the lifecycle.	Annex 11, 4.1	Yes. The PLM process includes all relevant documents. The responsibility for the validation of the application (see Annex 11, glossary) is with the regulated user.
4.1.4	A process for the validation of bespoke or customized systems should be in place.	Annex 11, 4.6	Customer-specific applications are verified in the scope of realization according to the responsibilities agreed upon in the project. The validation process is the responsibility of the regulated user.

4.1 Lifecycle and Validation of Computerized Systems

	Requirement	Reference	Answer
4.1.5	Change management and deviation management are applied during the validation process.	Annex 11, 4.2	Yes. The PLM process includes change management and deviation management. The regulated user should ensure appropriate change management and deviation management for customer-specific applications (see GAMP 5, appendices M8 and D5).
4.1.6	An up-to-date inventory of all relevant systems and their GMP functionality is available. For critical systems an up-to-date system description [...] should be available.	Annex 11, 4.3	The regulated user can use the standard product configuration reports of the SIMATIC SIPAT software. For any other software, operating systems, hosts and clients, the regulated user must establish appropriate reporting, a system inventory as well as system descriptions (see GAMP 5, appendix D6).
4.1.7	User Requirements Specifications should describe required functions, be risk-based and be traceable throughout the lifecycle.	Annex 11, 4.4	Yes. Specification of requirements is part of the PLM process. For the project-specific configuration, the regulated user must appropriately describe the user requirements in the system's lifecycle (see GAMP 5, appendix D1).
4.1.8	Evidence of appropriate test methods and test scenarios should be demonstrated.	Annex 11, 4.7	Ensuring the suitability of test methods and scenarios is an integral part of the PLM process. The regulated user should be involved to agree upon testing practice (see GAMP 5, appendix D5) for the customer-specific applications.
4.1.9	Appropriate controls should be used over system documentation. Such controls include the distribution of, access to, and use of system operation and maintenance documentation.	21 CFR 11.10 (k)	Yes. During the development of the product, the product's documentation is treated as being part of the product. As such, appropriate controls are ensured by the PLM process. The regulated user should establish appropriate procedural controls during development and operation of the system (see GAMP 5, appendices M9 and D6).
4.1.10	A formal change control procedure for system documentation maintains a time sequenced record of changes.	21 CFR 11.10 (k) Annex 11, 10	Yes. During the development of the product changes are handled according to the PLM process. The regulated user should establish appropriate procedural controls during development and operation of the system (see GAMP 5, appendices M8 and O6).
4.1.11	Persons who develop, maintain, or use electronic record/electronic signature systems should have the education, training and experience to perform their assigned task.	21 CFR 11.10 (i)	Yes. Siemens' processes do ensure that employees have appropriate training for their tasks and that such training is properly documented. Furthermore, Siemens offers a variety of training courses for users, administrators, and support staff.
4.1.12	Computerized systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP.	Annex 11, 11	The regulated user should establish appropriate procedural controls (see GAMP 5, appendices O3 and O8).

	Requirement	Reference	Answer
4.1.13	All incidents should be reported and assessed.	Annex 11, 13	To assist in the reporting and assessment of all incidents, all incidents related to and detected by the SIMATIC SIPAT system are logged in log files. The log files can be retrieved by users with proper access rights. The regulated user should establish appropriate procedural controls (see GAMP 5, appendix O5).
4.1.14	For the availability of computerized systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown.	Annex 11, 16	The regulated user should appropriately consider the system in its business continuity planning (see GAMP 5, appendix O10).

4.2 Suppliers and Service Providers

If the regulated user is partnering with third parties for planning, development, validation, operation and maintenance of a computerized system, then the competence and reliability of this partner should be considered utilizing a risk-based approach.

	Requirement	Reference	Answer
4.2.1	When third parties are used, formal agreements must exist between the manufacturer and any third parties.	Annex 11, 3.1	The regulated user is responsible to establish formal agreements with suppliers and third parties.
4.2.2	The competency and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.	Annex 11, 3.2 Annex 11, 4.5	The regulated user should assess its suppliers accordingly (see GAMP 5, appendix M2).
4.2.3	The regulated user should ensure that the system has been developed in accordance with an appropriate Quality Management System.	Annex 11, 4.5	The development of SIMATIC SIPAT follows the PLM process stipulated in the Siemens Quality Management System.
4.2.4	Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.	Annex 11, 3.3	The regulated user is responsible for the performance of such reviews.
4.2.5	Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.	Annex 11, 3.4	The content and extent of the documentation affected by this requirement should be agreed upon by the regulated user and Siemens. The joint non-disclosure agreement should reflect this requirement accordingly.

4.3 Data Integrity

4.3 Data Integrity

The main goal of both regulations is to define criteria under which electronic records and electronic signatures are as reliable and trustworthy as paper records. This requires a high degree of data integrity throughout the whole data retention period, including archiving and retrieval of relevant data.

	Requirement	Reference	Answer
4.3.1	The system should provide the ability to discern invalid or altered records.	21 CFR 11.10 (a)	Yes. An entry is generated in the audit trail for any user action. All relevant changes are recorded including time stamp, user ID, old value and new value. Depending on the configuration, a comment and meaning are also recorded. Unauthorized changes are prevented by the system through access control. Attached external documents, which might be added to records, are individually identified. Any alteration will be detected by the system.
4.3.2	For records supporting batch release, it should be possible to generate printouts indicating if any of the data has been changed since the original entry.	Annex 11, 8.2	Yes. By design, measured data cannot be modified. All operational modification of data and meta-data is recorded in the audit trail and can be printed out in a report.
4.3.3	The system should provide the ability to generate accurate and complete copies of electronic records in both human readable and electronic form.	21 CFR 11.10 (b) Annex 11, 8.1	Yes. All database records can be viewed through the SIMATIC SIPAT reports (provided as an option with the system) and the SIMATIC SIPAT Data Miner. Any other compatible database viewer can also be used. Electronic records, including audit trail, can be generated in PDF, Microsoft Excel, and ASCII forms which are immediately readable. Copies of the entire record can also be provided as an export. Configuration and runtime data can be inspected in the SIMATIC SIPAT client and Data Miner.
4.3.4	Computerized systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data.	Annex 11, 5	Yes. Depending on the type of data, such built-in checks include value ranges, data type check, access authorizations, checksums, etc. and finally the validation process including interface testing.
4.3.5	For critical data entered manually, there should be an additional check on the accuracy of the data.	Annex 11, 6	Yes. The system has built-in plausibility checks for data entry.
4.3.6	Data should be secured by both physical and electronic means against damage.	Annex 11, 7.1	In addition to the system's access security mechanisms, the regulated user should establish appropriate security means like physical access control, backup strategy, limited user access authorizations, regular checks on data readability, etc. Furthermore, the data retention period should be determined by the regulated user and appropriately considered in the user's processes (see GAMP 5, appendices O3, O4, O8, O9, O11 and O13).
4.3.7	Regular backups of all relevant data should be done.	Annex 11, 7.2	SIMATIC SIPAT supports automated backups. The regulated user should establish appropriate processes for backup and restore (see GAMP 5, appendix O9).

4.4 Audit Trail, Change Control Support

	Requirement	Reference	Answer
4.3.8	Electronic records must be readily retrievable throughout the records retention period.	21 CFR 11.10 (c) Annex 11, 17	Yes. Records stored in the SIMATIC SIPAT database can be accessed and exported through SIMATIC SIPAT Data Miner and the SIMATIC SIPAT reports. Exported data and reports must be securely stored by the regulated user to ensure retrievability throughout the retention period. It is the responsibility of the regulated user to use a correct export format for the report. Available formats include: XML, CSV and PDF. Backup functionality for securing all the records, recovery testing and maintaining the records throughout the retention period are customer responsibility.
4.3.9	If the sequence of system steps or events is important, then appropriate operational system checks should be enforced.	21 CFR 11.10 (f)	Yes. Standard processes and procedures for sequencing of steps and events exist in the system and are enforced through security controls. Predefined finite state mechanisms ensure this; furthermore, they include security protection making that only authorized personnel can perform manual state transitions. Others are prevented from performing the action. All state transitions are logged in the object's audit trail. Only objects with a status attributed with "GMP" are executable on a GMP station. In the default installation this is the "Approved" state. To acquire a status attributed with "GMP" for an object, an electronic signature is required.

4.4 Audit Trail, Change Control Support

During operation, regulations require the recording of operator actions that may result in the generation of new relevant records or the alteration or deletion of existing records.

	Requirement	Reference	Answer
4.4.1	The system should create a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data, the reason should be documented.	21 CFR 11.10 (e) Annex 11, 9	Yes. Changes during operation can be traced back by the system itself via audit trail and contain information with time stamp, user ID, old and new value, and comment. The audit trail is secure within the system and cannot be changed by a user. It can be made available and be exported in electronic portable document formats.
4.4.2	Management systems for data and documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.	Annex 11, 12.4	Yes. See also requirement 4.4.1.

4.5 System Access, Identification Codes and Passwords

	Requirement	Reference	Answer
4.4.3	Changes to electronic records shall not obscure previously recorded information.	21 CFR 11.10 (e)	Yes. Recorded information is not overwritten and is always available in the database.
4.4.4	The audit trail shall be retained for a period at least as long as that required for the subject electronic records.	21 CFR 11.10 (e) Annex 11, 9	Yes. This is technically feasible and must be considered in the application specific backup and restore process of the regulated user (see GAMP 5, appendices O9 and O13).
4.4.5	The audit trail should be available for review and copying by regulatory agencies.	21 CFR 11.10 (e)	Yes. See also requirement 4.4.1.

4.5 System Access, Identification Codes and Passwords

Since access to a system must be restricted to authorized individuals and the uniqueness of electronic signatures also depends on the authenticity of user credentials, user access management is a vital set of requirements regarding the acceptance of electronic records and electronic signatures.

	Requirement	Reference	Answer
4.5.1	System access should be limited to authorized individuals.	21 CFR 11.10 (d) 21 CFR 11.10 (g) Annex 11, 12.1	Yes. System access is based on Microsoft Windows user management. User rights are to be defined in the system. Nonetheless also procedural controls should be established by the regulated user, as described in GAMP 5, appendix O11.
4.5.2	The extent of security controls depends on the criticality of the computerized system.	Annex 11, 12.2	System security is a key factor during design and development of SIMATIC products. Nonetheless, since system security strongly depends on the operating environment of each IT system, these aspects should be considered in security management of the regulated user (see GAMP 5, appendix O11). Recommendations and support is given by Siemens' Industrial Security approach (http://www.siemens.com/industrialsecurity).
4.5.3	Creation, change, and cancellation of access authorizations should be recorded.	Annex 11, 12.3	Yes. Changes in user access management are recorded and should be subject to change control procedures of the regulated user.

4.5 System Access, Identification Codes and Passwords

	Requirement	Reference	Answer
4.5.4	If it is a requirement of the system that input data or instructions can only come from certain input devices (e.g. terminals), does the system check the validity of the source of any data or instructions received? (Note: This applies where data or instructions can come from more than one device, and therefore the system must verify the integrity of its source, such as a network of weigh scales, or remote, radio controlled terminals).	21 CFR 11.10 (h)	Yes. To prevent invalid data sources, the source of input data specifically and location of certain SIMATIC SIPAT components in general is configured in the system: all components are running on a so called SIMATIC SIPAT station. SIMATIC SIPAT stations define which PC is actually used and are configured in a controlled way as described above. The health of the communications is monitored and communications are confirmed using the TCP/IP protocol.
4.5.5	Controls should be in place to maintain the uniqueness of each combined identification code and password, so that no individual can have the same combination of identification code and password as any other.	21 CFR 11.300 (a)	SIMATIC SIPAT access is based on Microsoft Windows user management. The user ID and password are managed on an operating system level. User ID or password is not stored in any way on the local PC. Implementing and using the Microsoft Windows user management to prevent access to passwords without collaboration is the regulated user's responsibility.
4.5.6	Procedures are in place to ensure that the validity of identification codes is checked periodically.	21 CFR 11.300 (b)	The regulated user should establish appropriate procedural controls (see "Good Practice and Compliance for Electronic Records and Signatures, Part 2").
4.5.7	Passwords should periodically expire and have to be revised.	21 CFR 11.300 (b)	Password aging is a standard feature of the Microsoft Windows User Management. It is the regulated user's responsibility to implement it.
4.5.8	A procedure should be established for recalling identification codes and passwords if a person leaves or is transferred.	21 CFR 11.300 (b)	The regulated user should establish appropriate procedural controls (see "Good Practice and Compliance for Electronic Records and Signatures, Part 2"). The Microsoft Windows user management can be used to deactivate user accounts.
4.5.9	Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	21 CFR 11.300 (c)	Upon loss of a password, the Microsoft Windows account can be deactivated. Another user ID and password combination can be established to replace the lost ID/password. Deletions of users and modifications to the user's name are performed under procedural controls. The regulated user should establish appropriate procedural controls (see "Good Practice and Compliance for Electronic Records and Signatures, Part 2").

4.6 Electronic Signature

	Requirement	Reference	Answer
4.5.10	Measures for detecting attempts of unauthorized use and for informing security and management should be in place.	21 CFR 11.300 (d)	<p>Yes.</p> <p>Failed attempts to use the system or to perform electronic signatures are recognized and logged: All unsuccessful attempts are immediately notified to the user interface. Using the default installation of SIMATIC SIPAT, the user account is disabled after three unsuccessful attempts.</p> <p>The regulated user should establish appropriate procedural controls to ensure a periodic review of security and access control information logs (see GAMP 5, appendix O8).</p> <p>It is the SIMATIC SIPAT administrator's duty to unlock the user account if the account was locked by SIMATIC SIPAT.</p>
4.5.11	Initial and periodic testing of devices, such as tokens and cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	21 CFR 11.300 (e)	The regulated user should establish appropriate procedural controls (see "Good Practice and Compliance for Electronic Records and Signatures, Part 2").

4.6 Electronic Signature

To ensure that electronic signatures are generally accepted as equivalent to handwritten signatures executed on paper, requirements are not only limited to the act of electronically signing records. They also include requirements on record keeping as well as on the manifestation of the electronic signature.

	Requirement	Reference	Answer
4.6.1	Written policies should be established that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	21 CFR 11.10 (j) Annex 11, 14.a	The regulated user should establish appropriate procedural controls.
4.6.2	Signed electronic records should contain the following related information: <ul style="list-style-type: none"> • The printed name of the signer • The date and time of signing • The meaning of the signing (such as approval, review, responsibility) 	21 CFR 11.50 (a) Annex 11, 14.c	Yes. Signature manifestations contain the following information: <ul style="list-style-type: none"> • user ID (unique) and full user's name; • date and time (local and UTC); • the product functionality records what action was taken by the signer; • the meaning of the electronic signature (see comment below). Comment: The meaning of the electronic signature is selected from a drop-down list in the electronic signature window. The list of meanings for an applicable status transition is fully customizable by the regulated user. With a default SIMATIC SIPAT installation, no meanings are defined. In case meanings are present for a certain status transition, a value must be selected to perform the electronic signature. The selected meaning for the performed electronic signature is recorded. An additional field is provided for additional comments (notes) of the action. For example: In some situations, a comment can provide an explanation or details of the action.
4.6.3	The above-listed information is shown on displayed and printed copies of the electronic record.	21 CFR 11.50 (b)	Yes. The signature manifestations are protected in the same manner as the associated electronic record. The signature manifestations are viewable in SIMATIC SIPAT client and printable using the SIMATIC SIPAT reports.
4.6.4	Electronic signatures shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	21 CFR 11.70 Annex 11, 14.b	Yes. Signature manifestations are protected as electronic records and linked to the associated electronic record. Users cannot excise, copy, or otherwise falsify a manifestation of an electronic signature. Additional security measures should be taken to secure the SIMATIC SIPAT administrator privileges to the central database. This is the regulated user's responsibility.

4.6 Electronic Signature

	Requirement	Reference	Answer
4.6.5	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	21 CFR 11.100 (a) 21 CFR 11.200 (a) (2)	Yes. SIMATIC SIPAT access is based on Microsoft Windows user management. The user ID and password are managed on an operating system level. User ID or password is not stored in any way on the local PC. Implementing and using the Microsoft Windows user management correctly is the regulated user's responsibility. The re-use or re-assignment of electronic signatures is effectively prevented. Use of security roles in the product functionality negates the need to share passwords. Implementing policies against password sharing are the regulated user's responsibility.
4.6.6	When a system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batch.	Annex 11, 15	Electronic signatures are linked to an individual. The system allows strict determinations about which role and/or individual is allowed to perform a signature. It is the regulated user's responsibility to put the necessary controls in place to ensure only Qualified Persons are allowed to certify the release of the batches.
4.6.7	The identity of an individual should be verified before electronic signature components are allocated.	21 CFR 11.100 (b)	It is the regulated user's responsibility to establish appropriate procedural controls for the verification of an individual's identity before allocating a user account and/or electronic signatures.
4.6.8	When an individual executes one or more signings not performed during a single session, each signing shall be executed using all of the electronic signature components.	21 CFR 11.200 (a) (1) (ii)	Yes. Signings will require the re-entry of both electronic signature components, being login and password if the user does not perform the series of actions within a single session.
4.6.9	When an individual executes a series of signings during a single session, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one private electronic signature component.	21 CFR 11.200 (a) (1) (i)	Yes. Users log into a system to control system access, but this login is not used for the creation of an electronic signature (user ID must be re-entered first time electronic signature, password must always be re-entered).

	Requirement	Reference	Answer
4.6.10	The use of an individual's electronic signature by anyone other than the genuine owner would require the collaboration of two or more individuals.	21 CFR 11.200 (a) (3)	Yes. It is not possible to falsify an electronic signature during signing or after recording of the signature. In addition, the regulated user should establish appropriate procedural controls to prevent the disclosure of passwords. The system administrator has access to change passwords on operating system level. Additional security functionality is set up to limit an individual administrator's privileges (this is the regulated user's responsibility).
4.6.11	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owner.	21 CFR 11.200 (b)	Biometrics is outside the scope of the standard product offering.

4.7 Open Systems

The operation of an open system may require additional controls to ensure data integrity as well as the possible confidentiality of electronic records.

	Requirement	Reference	Answer
4.7.1	To ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records additional measures such as data encryption are used.	21 CFR 11.30	Yes. Encryption of the communication between services and between services and clients is implemented consistently.
4.7.2	To ensure the authenticity and integrity of electronic signatures, additional measures such as the use of digital signature standards are used.	21 CFR 11.30	SIMATIC SIPAT does not provide functionality for digital (encrypted) signatures.

4.7 Open Systems

Get more information

Siemens AG
Digital Industries
Pharmaceutical and Life Science Industry
Siemensallee 84
76187 Karlsruhe, Germany
PDF (A5E50732436-AA)
Produced in Germany

Subject to changes and errors. The information given in this catalog only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products.

The requested performance features are binding only when they are expressly agreed upon in the concluded contract. All product designations may be trademarks or product names of Siemens AG or other companies whose use by third parties for their own purposes could violate the rights of the owners.