SIEMENS

Solutions for Life Science

Electronic Records Assessment and GAMP® Software Categories

Desigo CC V3.0 - White Paper

CM110803_en
2017-10-24
Version 1

siemens.com/lifescience

Siemens Switzerland Ltd.
Building Technologies Division
International Headquarters
Gubelstrasse 22
CH-6301 Zug
Tel. +41 41-724 24 24

www.siemens.com/buildingtechnologies

Table of Contents

List of Tables

1. About this document

1.1 Scope and Objectives

Environmental monitoring systems must live up to the challenges of consistently complying with cGMP regulations that govern the use of computerized systems.

- EU GMP Annex 11
- US FDA 21 CFR Part 11
- Other regional equivalents, e.g. CFDA

This document defines the approach for each of the various components of the Desigo™ Building Management System (BMS) with regards to applicability and compliance with the above mentioned regulations.

- PX Automation Controller
- Desigo CC Management Station software

Further, this document reviews the GAMP® 5 Software Categories and defines how these can be applied to the various components for the Desigo BMS.

- Firmware
- Application Library
- Desigo CC Extension Modules and Graphic Libraries
- Project Specific bespoke applications

1.2 Before you start

1.2.1 Trademarks

The table below lists the trademarks used in this document listed together with their legal owners. The use of these trademarks is subject to international and national statutory provisions.

Trademarks	Legal owner
Desigo™	Siemens Switzerland Ltd.
GAMP®	International Society for Pharmaceutical Engineering Inc.
Microsoft … Windows Server® SQL® Server	Microsoft Corporation, see www.microsoft.com/trademarks
Adobe® and Acrobat®	Adobe Systems Incorporated, see http://www.adobe.com/ch_de/legal/permissions/trademarks.html

Table 1–1: Trademarks

All product names listed in the table are trademarks (™) or registered trademarks (®) of their respective owners, as listed in the table. With the exception of this section, these trademarks are not used elsewhere in the text (e.g. by use of symbols such as ® or ™) to facilitate reading of the text.

1.2.2 Copyright

1.2.3 Quality assurance

These documents have been prepared with great care. The contents of all documents are checked at regular intervals. Any corrections necessary are included in subsequent versions. Documents are automatically amended as a consequence of modifications and corrections to the products described. Please ensure that you have the latest revision date of the documentation. If you find any lack of clarity while using this document, or if you have any criticisms or suggestions, please contact your nearest branch office, or write directly to the support team at Headquarters in Zug (see below).

Support address:
Siemens Switzerland Ltd.
Building Technologies Division
International Headquarters
BT SSP SOL Life Science Center of Competence
Gubelstrasse 22
6301 Zug, Switzerland
Tel. +41 41 724 2424

Website: www.siemens.com/lifescience
Email: coc.pharma.sbt@siemens.com

1.2.4 Document use/request to the reader

Before using our solutions, it is important that you read carefully and in full the documents supplied with or ordered at the same time as the solution (equipment, applications, tools etc.). More information on the products and applications, e.g. system descriptions etc., are available on the Internet. We assume that the users of this solution and documents have the appropriate authorization and training, and that they are in possession of the technical knowledge necessary to use the solution in accordance with their intended application. If, despite this, there is a lack of clarity or other problems associated with the use of the documentation, please do not hesitate to contact your nearest branch office, or write directly to the support team at our Swiss headquarters. Email: coc.pharma.sbt@siemens.com.

Please note that without prejudice to your statutory rights, Siemens accepts no liability for any losses resulting from non-observance or improper observance of the points referred to above.

1.3 Document validity

This document is valid for projects using Desigo CC V3.0 Management Station. The descriptions in this document refer individual products within this release of the Desigo Building Management System.

1.3.1 Document revision history

The table below contains the revision history of this document. It does not give detailed change descriptions between versions, and serves only to ensure a correct correlation between the documentation and the product history that is documented in the respective datasheet.

Document Nr.	Doc. Version	Edition Date	Author	Remarks
CM110803en	1.0	24.10.2017	Tim Walsh	Desigo CC V3.0

Table 1–2: Document revision history

1.4 Target readers

This document contains information relevant for persons considering the mentioned systems for applications where compliance with ER/ES regulations is specified.

1.5 Document conventions

Caution — This symbol denotes information on safety instructions.

Warning — This symbol denotes information on warnings.

Tip — The symbol to the left denotes information that helps you properly operate and use the programs. This information is based on experience; we strongly suggest that you observe all hints.

Important note — Important information is printed on a gray background.

User or Supplier responsibility — Throughout the assessment chapter 5, the responsibility is defined in the column “Resp. U/S” whereby “U” refers to “User” being the end user of the system, for example, this would be the regulated company. And the definition “S” meaning “Supplier” refers to Siemens Building Technologies as supplier of the system at focus within this assessment.

2. General assessment details

2.1 Computer system use of ER & ES

This section describes the general details for the computer system(s) assessed for use of Electronic Records and Electronic Signatures.

PROJECT DETAILS			
Client	Siemens Building Technologies		
Project	Internal Audit of Building Management System Desigo CC Version 3.0	**Project Number**	n/a

ASSESSMENT DETAILS			
Assessment Requested by	Siemens Building Technologies	**Date of Assessment**	pending
Center of Competence Pharma	Timothy Walsh (Tpw) Vincenzo Ciccone (Vci)		
Client Personnel	n/a		
Supplier Personnel	n/a		

SYSTEM DETAILS			
System Name	Desigo CC Critical Monitoring Test Site	**System Serial No**	n/a
System Location	Total Building Solution Center, Zählerweg 9, 6301 Zug, Switzerland	**System Supplier**	Siemens Building Technologies
Application Software Title	Desigo CC V3.0, Desigo PXC100 Desigo DXR2.E17CX	**Program No./Revision**	Desigo CC V3.0, V3.0.0110.0 Desigo PXC100 FW V6.00.030 Desigo DXR2.E17 FW V1.21.29.104

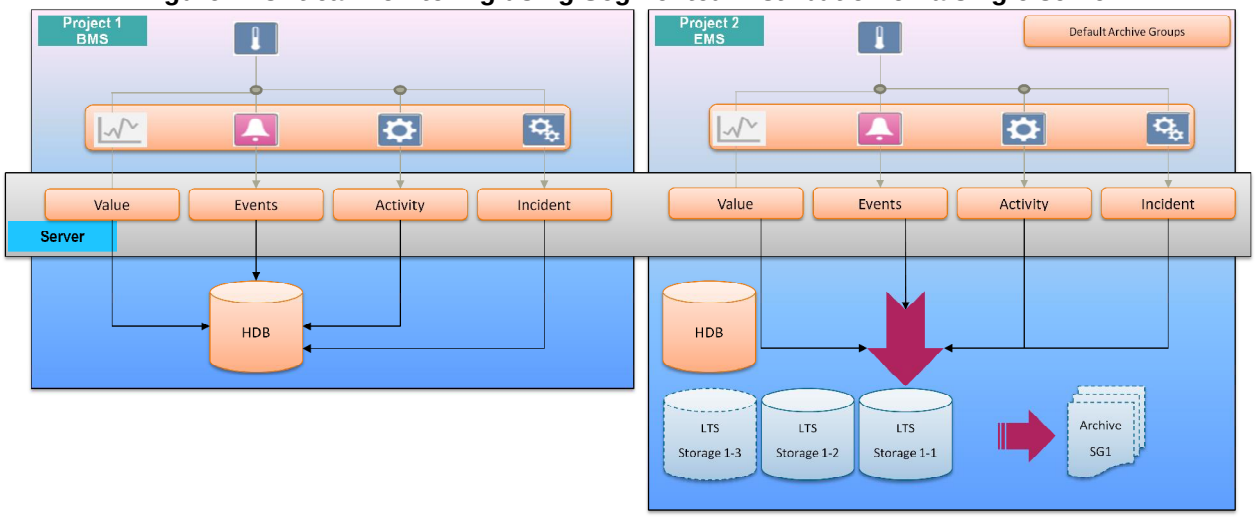
SYSTEM DESCRIPTION

There is one permanent test site for critical monitoring installed within the TBS Center in Zug using English language settings. It uses a Simatic Microbox PC running Microsoft Windows 2012 Server 64 bit operating system together with Desigo CC V3.0 Server. The Desigo CC is divided into two systems running on the same computer in a segmented distribution configuration, meaning that both systems run simultaneously on the same computer hardware. One system is defined as the non critical BMS and the other system is the EMS Monitoring critical part. The EMS system has been defined as the master which means that global users from the EMS system are able to view and modify values and properties also located on the non-critical BMS system according to their access levels and scopes. Whereas, vice-versa is intentionally not possible in this configuration.

The historical databases containing GMP data are located on the same computer hardware within a Microsoft SQL 2014 Express instance. The EMS system configuration is connected to one PXC100 which is

collecting trend data from several temperature and humidity sensors as well as a particle counter connected via ModBus/IP. The BMS system configuration is connected to one DXR2.E17CX controller which is running a pressurized room application for labs equipped with a fume hood that is connected to a simulation and test equipment rack.
In the following diagram we have shown how these two Desigo CC systems are setup on this site. All SQL databases exist within the same MS SQL instance and as you can see, the EMS side has configurations for long term storage of the GMP data.

Figure 1: Critical Monitoring using Segmented Distribution on a single server



3. Application of GAMP 5 Software Categories

3.1 Purpose of this chapter

The purpose of this chapter is to define the application of the GAMP software categories of the above mentioned Siemens Building Technologies software packages. This should help to define the proper validation approach for these systems when applied within the regulated industries.

The categories are based on the increasing risk of system failure and follow the progression from standard software to custom (bespoke) software.

Automated systems often consist of multiple components and within a single system these components may fall into various categories.

3.2 Scope of validity

The described definition can only be a recommendation as the final responsibility for the validation approach is always with the regulated company. This definition should be used as a basis of discussion with the Quality Assurance personnel on site and the results should be documented for each realized project. To quote the GAMP 5 Guide: "*These software categories [ ] may then be used along with Risk Assessment and Supplier Assessment to determine a suitable life cycle strategy. ".*

3.3 Allocation of Desigo BMS to GAMP Software Categories

With reference to GAMP 5 (2008), Appendix M4 "Categories of Software and Hardware", we make the following allocations for the above mentioned Desigo BMS software packages.

Cat.	Software Type	Application	Validation Approach	Remarks
1	Infrastructure Software	- Microsoft Windows 2012 Server - SQL 2014 Express - PX firmware	- Verify Name and Version (including service pack) during Verification. - The Operating System will be challenged indirectly by the functional testing of the application - Upgrade under change control - Access the impact of new, modified or removed features. - For non-configurable firmware, verify version during Verification. - Calibrate instruments as necessary during Verification. - Verify operation against requirements during Verification. - For configurable firmware, additionally verify the version and configuration. - Test functionality during Verification. - Manage custom (bespoke) firmware as category 5 software.	- Established commercially available operating systems. - Upgrades to the operating system could potentially lead to retesting of running applications. - The BT controllers have non-configurable firmware functions. The firmware is provided with the device. - If the firmware needs to be changed during the project this must be done in compliance with the customers change management process and the retesting effort should be investigated based on a risk analysis. - The functionality of the firmware is usually tested with the application. - The Verification needs updating if the revision of firmware is changed.
2	Removed from GAMP 5			

Cat.	Software Type	Application	Validation Approach	Remarks
3	Non-Configured Products	- Desigo CC V3.0 - PX Application Libraries	- Verify version (and configuration of environment) during Verification. - Test operation against user requirements during Verification. - Consider auditing the supplier for critical and complex applications. - Establish SOPs and training plans	- Category 3 covers off-the-shelf products that can either not be configured or products that can be configured, but for which only the default configuration is used. - Such packages have usually been installed in multiple industries and environments. - In Desigo CC this is the standard functionality, e.g. Log Viewer, Trend Viewer, Event List, Graphics Viewer, etc… - New versions are usually treated 'carefully' and risk assessment should be performed prior to upgrades being performed. - This software is usually tested with the project specific application. The validation effort is typically focused on the application (=individual configuration) of the software package (see category 4). - The development of these software packages was performed within a strictly controller quality management system that was audited by independent experts from the regulated industries. BT HQ Life Science CoC can provide copies of such vendor audit reports under provision of a non-disclosure agreement.

Cat.	Software Type	Application	Validation Approach	Remarks
4	Configurable Products	- Project specific configurations or libraries in Desigo CC - Configuration of PX application library elements - Standard protocol integrations at the Management Level (Desigo CC)	Requires validation plan for configuration and assessment of supplier. - Verify version (and configuration of environment) during Verification. - Test operation against user requirements during Verification. - Manage any custom (bespoke) programming as Category 5.	- The project specific application is usually based on the configuration of standard proven library elements. These are; the individual plant viewer graphic pages; the configuration of any alarm routing; the configuration of any reaction programs; the configuration of any report templates and the configuration of the software in the automation station. - If local libraries are used, it is mandatory to show the life cycle and the testing of these library elements so that the project specific application can be selected as Category 4. - The testing effort is mainly focused on the project specific applications. It is not necessary to test all functionality of the system – it is mandatory to test that the individual application requirements are fulfilled.
5	Custom Applications	- Project specific applications on Automation Level (PX) - Project specific drivers at the Management Level (Desigo CC), for example, using the Desigo CC API's.	- Requires validation plan addressing full life cycle - Validate complete system - Audit 3rd Party suppliers	- A complete life-cycle model approach for the development, testing and validation must always be completed for all custom built bespoke systems. - This can be, e.g. specific functionality on automation level or a project specific API interface in Desigo CC.

4. ER & ES Initial Assessment

This completed ER & ES initial assessment defines which of the subsequent parts of the detailed assessment must be completed for the system under assessment. This section has been completed based on commonalities between both 21 CFR Part 11 and EU GMP Annex 11 guidelines for use of Electronic Records and Electronic Signatures.

Step	Question	Response		Instruction
		Yes/No	Initial	
4.1.	Does the system store the GXP critical data on a durable medium (hard disk, floppy, tape etc.)?	Yes*	Vci/ Tpw	If YES – Goto Step 4.2. If NO – ER&ES Regulations do not apply to this system. Goto Chapter 6.
4.2.	Does the system create, modify, maintain, archive, retrieve or transmit in electronic form any record which must satisfy FDA record keeping requirements?	Yes*	Vci/ Tpw	If YES – Chapters 5.1, 5.2 and 5.4 must be completed. Goto Step 4.3. If NO – ER&ES Regulations do not apply to this system. Goto Chapter 6.
4.3.	Is the system an *Open* system?	No	Vci/ Tpw	If YES – Open system – Chapter 5.3 must be completed. Goto Step 4.4 If NO – Closed system – Chapter 5.3 not required. Goto Step 4.4
4.4.	Does this system use electronic signatures in place of hand-written signatures?	No**	Vci/ Tpw	If YES – Chapters 5.5 and 5.6 must be completed. Goto step 4.5. If NO – Chapters 5.5 and 5.6 not required. Goto step 4.5.
4.5.	Does the system use biometric signatures? (e.g. fingerprint, retinal scan etc.)	No	Vci/ Tpw	If YES – Chapter 5.7 must be completed. Goto Chapter 6. If NO – Chapter 5.7 is not required. Goto Chapter 6.

Comments:

* This assessment assumes that the Desigo system is monitoring GMP critical environments.

** Sections related to Electronic Signatures have been completed to show an example in case PDF reports generated by Desigo CC would be used by the regulated customer for electronic evidence submission to the authorities.

5. ER & ES Detailed Assessment

5.1 General Requirements

No.	Requirement	Resp. U/S	Part 11 Reference	Comment	Requirement Met?	
					Yes/No	Initial
5.1.1	**Validation**					
5.1.1.1	The system is validated. The scope of validation must include tests and checks which demonstrate compliance with all applicable parts of ER & ES Guidelines.	U	11.10 (a)	**Desigo System components:** The system and its applications can be validated. Note that the application must be validated within the scope of an individual project. For this purpose Siemens offers comprehensive validation support, but - given by regulation - the end user will always have the final responsibility for the project specific validation.	Yes	Vci/ Tpw

No.	Requirement	Resp. U/S	Part 11 Reference	Comment	Requirement Met?	
					Yes/No	Initial
5.1.2	**Training**					
5.1.2.1	Staff that ***developed*** the electronic record/signature system are properly trained & experienced. NOTE: Training records should be available for review.	S	11.10 (i)	**Desigo System components:** All Desigo System components are developed within the CPS R&D organization which achieved CMMI level 3.0 in 2010. CMMI 3.0 includes the process area of Organization Training (OT). The purpose of OT is to develop skills and knowledge of people so that they can perform their roles effectively and efficiently. The process is in place since 2007 and has been improved continuously. The process followed first defined a top down view of all roles and core competencies required for our business. Then, in a bottom up process, each employee was assessed and mapped to roles. Any deviations in competencies are then continuously addressed as part of the annual performance review between employee and manager. Life Science specific trainings are offered and executed by the BT Academy and tracked for each employee.	Yes	Vci/ Tpw
5.1.2.2	Staff that ***maintain*** the electronic record/signature system are properly trained & experienced. NOTE: This includes system administrators, database administrators, etc. Training records should be available for review.	U	11.10 (i)	**Desigo System components:** Not applicable – system user will decide who maintains the system.	n/a	Vci/ Tpw
5.1.2.3	Staff that ***use*** the electronic record/signature system are properly trained & experienced. NOTE: Training records should be available for review.	U	11.10 (i)	**Desigo System components:** Not applicable – system user responsibility.	n/a	Vci/ Tpw

No.	Requirement	Resp. U/S	Part 11 Reference	Comment	Requirement Met?	
					Yes/No	Initial
5.1.3	**Documentation**					
5.1.3.1	Adequate documentation is available to describe the ***maintenance*** of the system. NOTE: This includes SOP's.	U	11.10 (k) (1)	**Desigo System components:** SOPs available from Siemens if required by customer. (NOT reviewed as part of this assessment).	Yes	Vci/ Tpw
5.1.3.2	Adequate documentation is available to describe the ***use*** of the system. NOTE: This includes SOP's.	U	11.10 (k) (1)	**Desigo System components:** Full set of user documentation exists that include (but is not limited to); - Installation and Engineering Guides - System Descriptions - User Guides - Customer Training Guides SOPs are user responsibility.	Yes	Vci/ Tpw
5.1.3.3	The distribution of system documentation is controlled, i.e. is available only to those individuals who require it.	U	11.10 (k) (1)	**Desigo System components:** Not applicable – system user responsibility.	n/a	Vci/ Tpw
5.1.3.4	System documentation is produced and maintained under a revision control procedure.	U	11.10 (k) (2)	**Desigo System components:** Applicable for standard system documentation provided by Siemens. Project specific documentation (e.g. SOPs, validation documents) is in the responsibility of the system owner.	Yes	Vci/ Tpw

No.	Requirement	Resp. U/S	Part 11 Reference	Comment	Requirement Met?	
					Yes/No	Initial
5.1.4	**System Security**					
5.1.4.1	System access is limited to authorized individuals. NOTE: This will normally be by entry of correct ID/password combination.	S	11.10 (d)	**Desigo PXC:** Local access security to the automation station is based on User ID and password combination. Users at the local automation station level are not synchronized with the management station.	Yes	Vci/ Tpw
				Desigo CC: Desigo CC users can be configured to use local passwords or to use Windows authentication (for example, Active Directory). Use Windows authentication wherever possible to enhance security, control, and management of passwords.	Yes	Vci/ Tpw
5.1.4.2	Authority checks are in place to restrict specific system functions to authorized individuals. NOTE: This will normally be by definition of user groups or roles, defining specific permissions to each role and then assigning users to one or more groups.	S	11.10 (g)	**Desigo PXC and Desigo CC:** Users are assigned to different standard groups (e.g. operator, engineer, service, etc – more groups are configurable if required). Within groups individual functions and applications can be assigned or removed for this specific group. It is possible to restrict individual user's access to specific data points.	Yes	Vci/ Tpw
5.1.4.3	An approved procedure which describes the administration of security is available which includes: 1. Add new user. 2. Assign user to groups/roles. 3. Change user privileges. 4. Retire (but not delete, see 5.1.4.4) user. 5. Force reissue of password.	U	11.10 (d)	**Desigo System components:** Applicable for standard system documentation provided by Siemens. Project specific documentation (e.g. SOPs, validation documents) is in the responsibility of the system owner.	Yes	Vci/ Tpw

No.	Requirement	Resp. U/S	Part 11 Reference	Comment	Requirement Met?	
					Yes/No	Initial
5.1.4.4	To ensure uniqueness of user ID's, users should never be deleted from the system. Instead the ID should be 'deactivated' but retained.	U	11.10 (d)	**Desigo PXC:** PXC does not provide the option "deactivate user". Due to this reason in GxP application the user operation should always be with Desigo CC.	No	Vci/ Tpw
				Desigo CC: Managed by Windows Authentication (Active Directory). Also local Desigo CC user accounts can be enabled or disabled by an administrator.	Yes	Vci/ Tpw
5.1.5	**Operational Checks**					
5.1.5.1	The system forces a permitted sequencing of steps and events. NOTE: This is system dependent. An enforced sequence of operations may not be required. If this subpart is not applicable, record the reason in the comments section.	S	11.10 (f)	**Desigo PXC:** Not applicable – there are no enforced sequences of operations.	n/a	Vci/ Tpw
				Desigo CC: Partly applicable – in general there are no enforced sequences of operations. Enforcing a sequencing of steps is possible for alarm management and forced commenting of actions.	Yes	Vci/ Tpw

No.	Requirement	Resp. U/S	Part 11 Reference	Comment	Requirement Met?	
					Yes/No	Initial
5.1.6	**Device Checks**					
5.1.6.1	Device checks are used to determine the source of data or operational instruction.	S	11.10 (h)	**Desigo PXC:** The communication with the automation stations as a source of data is continuously supervised. The communication with the Input and Outputs as a source of data is continuously supervised. Each new value from physical data point receives a dedicated quality attribute which informs about the integrity and status of the information. Field connected devices are verified by routine loop calibration verifying the accuracy of the sensor and corresponding recorded data.	Yes	Vci/ Tpw
				Desigo CC: System devices have unique addresses which are verified as part of the commissioning and qualification process. Data for these devices may only be collected by the system (user does not have the ability to enter or modify collected data). Client software must be installed on a workstation to access the system. Certificates must be exchanged between client and server in order for a client to be able to access a project.	Yes	Vci/ Tpw

5.2 Electronic Record Requirements

No.	Requirement	Resp. U/S	Part 11 Reference	Comment	Requirement Met?	
					Yes/No	Initial
5.2.1	**Record Management**					
5.2.1.1	Accurate copies of electronic records (including audit trails) can be made in both paper and electronic form. NOTE: Electronic copies should be in a standard format e.g. ASCII file, MS Office document or XML.	S	11.10 (b) 11.10 (e)	**Desigo PXC:** PXC handles only transient data. The ERs are securely stored in Desigo CC databases. The operation of PXC automation stations in GxP applications is only with Desigo CC.	Yes	Vci/ Tpw
				Desigo CC: All ERs are stored in SQL databases – including the audit trail. It is possible to generate accurate copies of the ERs in paper, PDF, or XML format protected for integrity with checksums which can easily be verified.	Yes	Vci/ Tpw
5.2.1.2	An approved procedure which describes the process of making these copies is available.	U	11.10 (b)	**Desigo System components:** Not applicable. Is in the responsibility of the user.	n/a	Vci/ Tpw
5.2.1.3	Electronic records (including audit trails) are backed-up on a regular basis.	U	11.10 (c) 11.10 (e)	**Desigo PXC:** PXC handles only transient data, therefore, this is not applicable.	n/a	Vci/ Tpw
				Desigo CC: Complete project backup (configuration and data) either manually or scheduled. Complete data backup of SQL databases at fixed intervals (hourly, daily, weekly).	Yes	Vci/ Tpw
5.2.1.4	An approved procedure which describes the backup process is available.	U	11.10 (c)	**Desigo System components:** Not applicable. Is the responsibility of the user.	n/a	Vci/ Tpw

No.	Requirement	Resp. U/S	Part 11 Reference	Comment	Requirement Met?	
					Yes/No	Initial
5.2.1.5	Electronic records (including audit trails) can be archived for long term storage and are fully retrievable. NOTE: This should be designed to retain the record for the period required by the predicate rule.	S/U	11.10 (c) 11.10 (e)	**Desigo PXC:** Changes made to programs loaded into the controller are tracked through customer SOP. Other changes are tracked by Desigo CC audit trails.	n/a	Vci/ Tpw
				Desigo CC: Desigo CC archives audit, trend and log data either manually or automatically for long term storage. Archives which have been taken offline can easily be returned online providing they are accessible to the Desigo CC Server.	Yes	Vci/ Tpw
5.2.1.6	Approved procedures which describe the archive and restore process are available.	S/U	11.10 (c)	**Desigo CC:** Desigo CC standard documentation describes the functionality, however, site specific SOPs are the User's responsibility.	Yes	Vci/ Tpw
5.2.1.7	The retention period for the electronic records created by the system is clearly defined.	U	11.10 (c)	**Desigo System components:** Not applicable – system user responsibility.	n/a	Vci/ Tpw
5.2.2	**Audit Trails**					
5.2.2.1	Creation, modification and deletion of any electronic record covered by the rule results in the creation of an entry in an audit trail.	S	11.10 (e)	**Desigo PXC:** The Desigo PXC does not record changes made directly at the controller. Creation, modification or deletion of records are completed through Desigo CC or system tools which will provide audit trail.	n/a	Vci/ Tpw
				Desigo CC: Any changes of ERs (create, modify, delete) are stored in the Desigo CC databases (old value, new value, date, time, user and comment). These databases are secured with standard SQL database security measures.	Yes	Vci/ Tpw

No.	Requirement	Resp. U/S	Part 11 Reference	Comment	Requirement Met?	
					Yes/No	Initial
5.2.2.2	The audit trail is generated automatically by the system.	S	11.10 (e)	**Desigo PXC:** PXC covers only transient data and does not possess an audit trail.	n/a	Vci/ Tpw
				Desigo CC: User and System activity logging cannot be switched off.	Yes	Vci/ Tpw
5.2.2.3	Each audit trail entry consists of:	S	11.10 (e)	**Desigo PXC:** PXC covers only transient data and does not possess an audit trail.	n/a	Vci/ Tpw
	1. Operator ID.	S	11.10 (e)	**DesigoCC:** User name. In case Windows authentication is used, then the qualified Windows Domain Username is recorded.	Yes	Vci/ Tpw
	2. Action performed.	S	11.10 (e)	**Desigo CC:** Event category	Yes	Vci/ Tpw
	3. New and previous values if the action is modify/update.	S	11.10 (e)	**Desigo CC:** Previous value and new value are stored together with the ER in the history database.	Yes	Vci/ Tpw
	4. Time and date action occurred.	S	11.10 (e)	**Desigo CC:** Date/Time	Yes	Vci/ Tpw
5.2.2.4	Access to the audit trail is read-only through any standard system function.	S	11.10 (e)	**Desigo PXC:** PXC covers only transient data and does not possess an audit trail.	n/a	Vci/ Tpw
				Desigo CC: The history database is readable with the application *Log Viewer or via Reports* – no changes are possible.	Yes	Vci/ Tpw

No.	Requirement	Resp. U/S	Part 11 Reference	Comment	Requirement Met?	
					Yes/No	Initial
5.2.2.5	An approved procedure which describes the method of maintaining the accuracy of system clocks which perform time-stamping is available. This should include the regular synchronization of system clocks if appropriate.	U	11.10 (e)	**Desigo System components:** Not applicable – system user responsibility. Time is synchronized throughout the system automatically at fixed intervals. Additionally, PC base software can have time synchronized through network time servers if available.	n/a	Vci/ Tpw
5.2.2.6	Modification of system time should be restricted to authorized users only.	S/U	11.10 (e)	**Desigo System components:** All operations of the automation stations are restricted to the assigned user groups. The system time is provided and synchronizes via Desigo CC. Windows time is used for audit trails and events. Access restriction to Windows server clock is a system administrator responsibility.	Yes	Vci/ Tpw

5.3 Open System

IMPORTANT NOTE: If this system is classified as Open then seek additional guidance if required to complete this section.

No.	Requirement	Resp. U/S	Part 11 Reference	Comment	Requirement Met?	
					Yes/No	Initial
5.3.1.1	In addition to those requirements identified in sections 5.1 and 5.2, the system has additional controls which may include: • Data Encryption • Digital Signatures	S	11.30	**Desigo System components:** Desigo is a closed system	n/a	Vci/ Tpw

5.4 Signature Manifestations and Signature/Record Linking

No.	Requirement	Resp. U/S	Part 11 Reference	Comment	Requirement Met?	
					Yes/No	Initial
5.4.1	**Signature Manifestations**					
5.4.1.1	The electronic signature contains the following components: • The printed name of the signer. • The time and date the signature was made. • The meaning of the signature e.g. Approved, Rejected	S	11.50 (a)	**Desigo System components:** Not applicable – the Desigo system does not support electronic submission of quality relevant data to the regulating authorities. If submission uses paper copies, then the user must add an approved signature. PDF reports generated from Desigo CC support the inclusion of Digital Signatures, e.g. Adobe Acrobat plug-in. These signatures support many features including printed name of the signer, signature date, reason for signing, location, labels, logos and other parameters.	n/a	Vci/ Tpw
5.4.1.2	The electronic signature components identified in sections 5.4.1.1 above are visible on any form of the electronic record to which they are associated. NOTE: This includes printouts and screen displays.	S	11.50 (b)	**Desigo System components:** Not applicable – Desigo does not use or deploy electronic signatures.	n/a	Vci/ Tpw

No.	Requirement	Resp. U/S	Part 11 Reference	Comment	Requirement Met? Yes/No	Initial
5.4.2	**Signature/Record Linking**					
5.4.2.1	Each electronic signature is linked to it's associated electronic record to ensure that the signature cannot be excised, copied, transferred or in any way falsified *by ordinary means.* NOTE: There must no access to electronic signatures other than read only via the standard system functions. Any other access to records containing signatures must be restricted. Any legitimate access to such records (e.g. by a database administrator) must be restricted by procedure.	S	11.70	**Desigo System components:** Not applicable – Desigo does not use or deploy electronic signatures.	n/a	Vci/ Tpw

5.5 Electronic Signature General Requirements

This section applies to both biometric and non-biometric electronic signatures.

No.	Requirement	Resp. U/S	Part 11 Reference	Comment	Requirement Met? Yes/No	Initial
5.5.1	**Policies**					
5.5.1.1	A written policy is available that holds individuals accountable and responsible for actions initiated by their electronic signature. Records are available to confirm that all electronic signature users have read and understood this policy.	U	11.10 (j)	**Desigo System components:** Not applicable – Desigo does not use or deploy electronic signatures. System user responsibility.	n/a	Vci/ Tpw

No.	Requirement	Resp. U/S	Part 11 Reference	Comment	Requirement Met? Yes/No	Initial
5.5.1.2	A letter has been sent to the FDA by the user, stating the intent to use electronic signatures prior to first use of the system.	U	11.100 (c)	**Desigo System components:** Not applicable – Desigo does not use or deploy electronic signatures. System user responsibility.	n/a	Vci/ Tpw
5.5.2	**Electronic Signature Issue**					
5.5.2.1	Each electronic signature is unique to one individual and shall not be reused by or reassigned to anyone else.	U	11.100 (a)	**Desigo System components:** Not applicable – Desigo does not use or deploy electronic signatures. System user responsibility.	n/a	Vci/ Tpw
5.5.2.2	No shared/group accounts are defined as electronic signatures.	U	11.100 (a)	**Desigo System components:** Not applicable – Desigo does not use or deploy electronic signatures. System user responsibility.	n/a	Vci/ Tpw
5.5.2.3	The identity of each individual must be verified prior to use of an electronic signature. NOTE: A practical interpretation is that the individual is authorized by their manager to be issued with an electronic signature.	U	11.100 (b)	**Desigo System components:** Not applicable – Desigo does not use or deploy electronic signatures. System user responsibility.	n/a	Vci/ Tpw
5.5.2.4	An approved procedure which describes the administration of electronic signatures is available and includes: • Issue of electronic signatures. • Withdrawal of electronic signatures. • Loss management procedures.	U	11.100 (a) 11.100 (b) 11.300 (c)	**Desigo System components:** Not applicable – Desigo does not use or deploy electronic signatures. System user responsibility.	n/a	Vci/ Tpw

5.6 Non-Biometric Electronic Signature Requirements

This section applies to the use of ID password or token/password combinations.

No.	Requirement	Resp. U/S	Part 11 Reference	Comment	Requirement Met?	
					Yes/No	Initial
5.6.1	**Non-Biometric Signature Use**					
5.6.1.1	The electronic signature consists of two distinct identification components. NOTE: in practice this will be either: • User ID/password. • Token (e.g. ID Swipe Card)/password.	S	11.200 (a) (1)	**Desigo System components:** Not applicable – Desigo does not use or deploy electronic signatures. System user responsibility.	n/a	Vci/ Tpw
5.6.1.2	The first signing in a single period of controlled system access must use both signature components.	S	11.200 (a) (1) (i)	**Desigo System components:** Not applicable – Desigo does not use or deploy electronic signatures. System user responsibility.	n/a	Vci/ Tpw
5.6.1.3	Subsequent signings in the same session may use one component only. NOTE: This is an optional requirement but if used then the component must be the secure part i.e. the password.	S	11.200 (a) (1) (i)	**Desigo System components:** Not applicable – Desigo does not use or deploy electronic signatures. System user responsibility.	n/a	Vci/ Tpw
5.6.1.4	Multiple signings not performed in a single period of controlled system access must all use both components.	S	11.200 (a) (1) (ii)	**Desigo System components:** Not applicable – Desigo does not use or deploy electronic signatures. System user responsibility.	n/a	Vci/ Tpw
5.6.1.5	The electronic signature must be used only by the genuine owner.	S	11.200 (a) (2)	**Desigo System components:** Not applicable – Desigo does not use or deploy electronic signatures. System user responsibility.	n/a	Vci/ Tpw
5.6.1.6	The password component of an electronic signature is not visible to any system user including the administrator.	S	11.200 (a) (3)	**Desigo System components:** Not applicable – Desigo does not use or deploy electronic signatures. System user responsibility.	n/a	Vci/ Tpw

No.	Requirement	Resp. U/S	Part 11 Reference	Comment	Requirement Met?	
					Yes/No	Initial
5.6.2	**Non-Biometric Signature Maintenance**					
5.6.2.1	A signature ID must never be deleted, only retired, to ensure that it is always unique.	S/U	11.300 (a)	**Desigo System components:** Not applicable – Desigo does not use or deploy electronic signatures. System user responsibility.	n/a	Vci/ Tpw
5.6.2.2	The system will prevent creation of a User ID that has been previously defined.	S	11.300 (a)	**Desigo System components:** Not applicable – Desigo does not use or deploy electronic signatures. System user responsibility.	n/a	Vci/ Tpw
5.6.2.3	The password component of an electronic signature periodically expires and must be changed by the user.	S	11.300 (b)	**Desigo System components:** Not applicable – Desigo does not use or deploy electronic signatures. System user responsibility.	n/a	Vci/ Tpw
5.6.2.4	System must detect & report any attempts at unauthorized access. NOTE: This could be by writing an entry in a security log if 3 consecutive, unsuccessful attempts are made to make an electronic signature.	S	11.300 (d)	**Desigo System components:** Not applicable – Desigo does not use or deploy electronic signatures. System user responsibility.	n/a	Vci/ Tpw
5.6.2.5	An approved procedure which describes the monitoring of electronic signature violations and the actions to take should be available.	U	11.300 (d)	**Desigo System components:** Not applicable – Desigo does not use or deploy electronic signatures. System user responsibility.	n/a	Vci/ Tpw
5.6.2.6	Tokens are periodically tested, following an approved procedure, to ensure they function correctly and have not been tampered with. NOTE: Not applicable to User ID/password combinations.	U	11.300 (e)	**Desigo System components:** Not applicable – Desigo does not use or deploy electronic signatures. System user responsibility.	n/a	Vci/ Tpw

5.7 Biometric Electronic Signature Requirements

This section applies to biometric signatures only – seek additional guidance if required to complete this section.

No.	Requirement	Resp. U/S	Part 11 Reference	Comment	Requirement Met?	
					Yes/No	Initial
5.7.1.1	The signature system is designed so that each signature can only be used by its genuine owner.	S	11.200 (b)	**Desigo System components:** Not applicable – Desigo does not use or deploy biometric signatures. System user responsibility.	n/a	Vci/ Tpw

6. Assessment Summary

Step				Comments
		Yes/No	Initial	
6.1.1.1	Do regulations governing Electronic Records apply to this system?	Yes	Vci/ Tpw	**Desigo System components** Records are captured and securely stored by the Desigo System
6.1.1.2	Is this an Open system?	No	Vci/ Tpw	
6.1.1.3	Does the system use electronic signatures?	No	Vci/ Tpw	**Desigo CC:** Digital signatures can be used, for example, based on PDF reports created and signed by Adobe Acrobat plug-in. This strategy supports a goal of meeting the FDA's guidance for electronic submissions, which recommends only Adobe Acrobats default plug-ins.
6.1.1.4	If Yes, are Biometric signatures used?	No	Vci/ Tpw	
6.1.1.5	Is the system fully compliant with ER&ES regulations like, 21 CFR Part 11 or EU Annex 11?	Yes	Vci/ Tpw	**Desigo CC:** All technical 21 CFR Part11 requirements are fulfilled excluding Electronic Signatures. Also, capture of “reason for change” is supported using Desigo CC Validation Profile configuration. Digital Signatures are possible using Adobe Acrobat and PDF reports generated by the system.

Siemens Switzerland Ltd
Building Technologies Division
International Headquarters
Gubelstrasse 22
6301 Zug
Switzerland
Tel +41 41 724 24 24

Answers for infrastructure and cities.
Our world is undergoing changes that force us to think in new ways: demographic change, urbanization, global warming and resource shortages. Maximum efficiency has top priority – and not only where energy is concerned. In addition, we need to increase comfort for the well-being of users. Also, our need for safety and security is constantly growing. For our customers, success is defined by how well they manage these challenges. Siemens has the answers.

“We are the trusted technology partner for energy-efficient, safe and secure buildings and infrastructure.”

siemens.com/lifescience
Restricted