06 / 2024

Assessment of Regulatory Compliance of Lucullus® Regarding 21 CFR Part 11

1 INTRODUCTION

To ensure product quality within bioprocess-based manufacturing, more and more process analytic technology, computerized systems, electronic devices and software are applied. This results in a replacement of paper-based documentation to electronic documentation. To further ensure quality management, the United States Food and Drug Administration (FDA) has defined regulatories, which describe the requirements of computerized systems within the lifecycle of pharmaceutical products. The regulation 21 CFR Part 11 "Electronic Records; Electronic Signatures" sets forth the criteria under which electronic records, electronic signatures, and handwritten signatures executed to electronic records can be considered trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper. This applies to records in electronic form that are created, modified, maintained, archived, retrieved or transmitted. This requirement aims to guarantee the quality of the manufactured product by ensuring that electronic records are always complete, reliable and accurate. The regulations describe and require multiple levels of control. The software itself is a technological solution with many available features which can be used/configured to comply with these control levels. It is the responsibility of the customer to ensure their correct implementation.

Regarding to 21 CFR Part 11, Lucullus® (Process Information Management System) is a recording system. As shown in the next sections, Lucullus® can be configured to comply with the key requirements of 21 CFR Part 11.

This document comprises the following three parts:

i. Overview of 21 CFR Part 11 requirements
ii. Lucullus® solutions for main technical requirements of 21 CFR Part 11
iii. Detailed evaluation of Lucullus®

2 OVERVIEW OF FDA 21 CFR PART 11 REQUIREMENTS

These chapter summaries the most important technical requirements of the 21 CFR Part 11. The overall goal of the technical requirements for electronic records and electronic signatures is to prevent manipulation of data. The following Table 1 sum up the key requirements of recording systems.

Table 1: Summary of key requirements of recording systems according to FDA 21 CFR Part 11

REQUIREMENT	DESCRIPTION	RESPONSIBILITY
Validation	Recording systems must be validated to ensure precise, reliable and consistent data management and the ability to discern invalid or altered records.	Customer
Audit trail	All operator actions which create, modify or delete an electronic data record must be recorded in a timestamped, computer generated and secure audit trail.	Securecell AG
Access protection	Access to electronic records must be limited to authorized and qualified users. Additional security procedures must be implemented for open systems	Securecell AG
Record retention, protection, reproducibility & retrievability	The recording systems must have the capability to retain, protect and readily retrieve records during the required retention period. Systems must be able to reproduce electronic reports in both human-readable and electronic form.	Customer & Securecell AG
System documentation	Controls must be in place over the distribution of, access to, and use of documentation for system operation and maintenance.	Securecell AG & Customer
Electronic signature	Systems must allow to control that use of an electronic signature is limited to genuine owners only and that attempted use by others is promptly detected and recorded. Non-biometric systems must employ two distinct identification mechanisms (user ID/password). Both user ID and password must be entered before the signature is made, and at least the password must be entered at each subsequent signing during the same session. Electronic signatures must not be reused or reassigned. The purpose of an electronic signature must be clearly indicated. Falsification of electronic signatures must be prevented by the system. Electronic signatures must be legally binding and equivalent of the user's handwritten signature.	Securecell AG
Certificate to FDA	Written certification must be provided to the FDA Office of Regional Operations that all electronic signatures in use are the legally binding equivalent of traditional handwritten signatures.	Customer

3 LUCULLUS® SOLUTIONS FOR 21 CFR PART 11 REQUIREMENTS

The 21 CFR Part 11 requirements of recording systems, such as the software Lucullus®, can be addressed in four main topics:

i. Access Security
ii. Electronic signature
iii. Audit trail
iv. Archiving and retrieval

Within the next paragraphs, the implemented technical solutions to support 21 CFR Part 11 compliance with regard to those four topics will be presented.

3.1 Access Security

Access to Lucullus® and specific functionalities is controlled by the combination of access protection and extensive user management. Following requirements for access protection are met by Lucullus®:

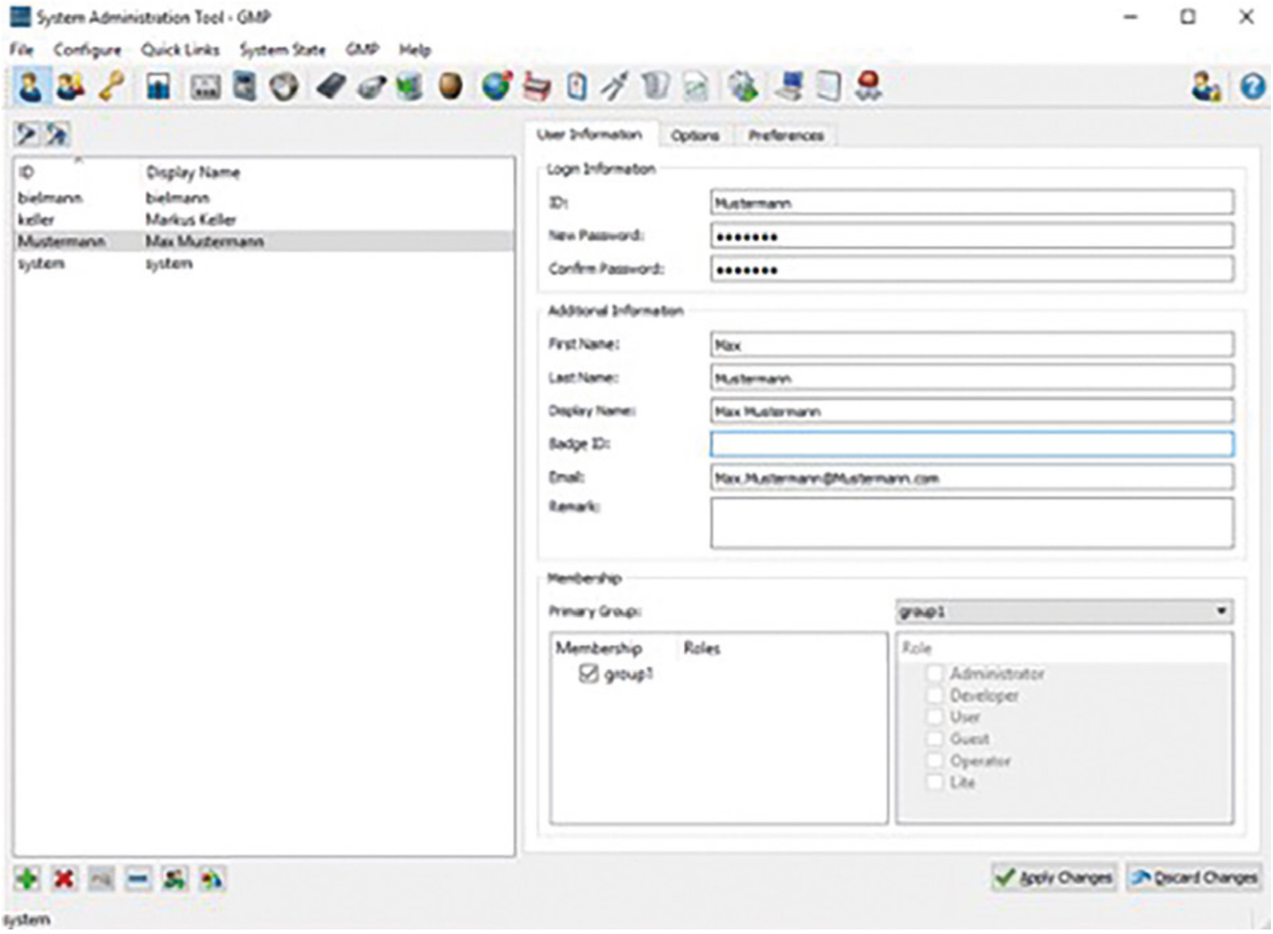
a) User login with a unique combination of user ID and password
b) The user can be forced to change the initial password
c) User can change their own password
d) Password security settings that can be defined by the customer:
 - Minimum password length
 - Password expiration with a validity period of the password and the number of generations can be defined by the customer.
e) The user is automatically blocked after three incorrect login attempts and can only be unlocked by the administrator
f) The system automatically logs off users after a specified time period
g) Log functions and actions related to access protection in the audit trail, such as login, manual and automatic logoff, input of wrong user ID or wrong password, user blocked after costumer defined number of failed login attempts.

In addition to controlled user access, Lucullus® provides extensive user management on two levels: individual users have "roles" with definable access rights and individual users are assigned to "groups" with specific resources.

Lucullus® provides default user roles (administrator, developer, operator and guest) which can be modified according to the rights. Roles are defined by a set of rights which can be adapted by an administrator. Specific rights are listed in Table 2.

Table 2: Summary and description of rights in Lucullus®

RIGHTS	DESCRIPTION
Login	Right to Login
View processes	Loading and viewing processes
Start/stop operations	Starting and stopping data logging
Enter offline data	Entering offline data
Alter log list	Changing the port properties in the Online Tool
Setpoint changes	Changing setpoints in the Online Tool
Data Management Tool	Functions of the Data Management Tool without the permission to delete data and processes
Configure reports	Creating and editing report templates
Configure reactors	Configuring reactors
Configure devices	Configuring devices, subdevices and ports
Configure users	User administration
Online step chain	Manual step jumps in the step chain in the Online Tool
Operation Tool	Usage of the Operation Tool
DBInterface admin	Database interface administration
DBInterface user	Database interface user
Media Tool master	Managing the Media Tool
Media Tool user	Media Tool user
Media Tool configuration	Configuring the Media Tool
Media stock user	Media storage user
Media stock admin	Managing the media storage
Monitoring user	Monitoring users
Application settings admin	Managing application settings



ID	Display Name
bielmann	bielmann
keller	Markus Keller
Mustermann	Max Mustermann
system	system

Login Information

ID: Mustermann

New Password: •••••••

Confirm Password: •••••••

Additional Information

First Name: Max

Last Name: Mustermann

Display Name: Max Mustermann

Badge ID:

Email: Max.Mustermann@Mustermann.com

Remark:

Membership

Primary Group: group1

Membership	Roles
☑ group1	

Role

- □ Administrator
- □ Developer
- □ User
- □ Guest
- □ Operator
- □ Lite

system

Figure 3.1: User Interface of Lucullus® for defining user roles. Each role consists of a collection of access rights

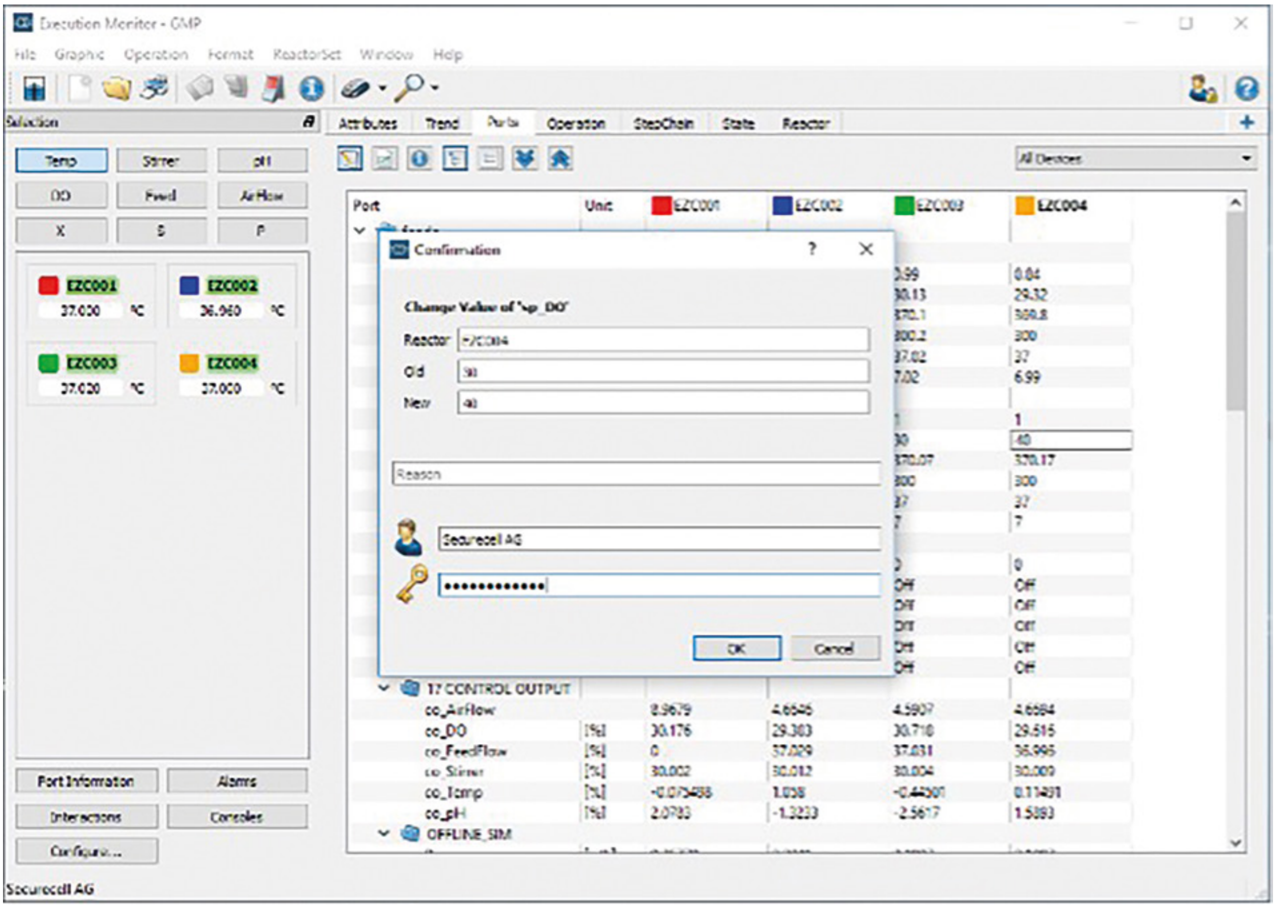
3.2 Electronic Signatures

Within the listed versions of Lucullus® (see chapter 5), all interactions around a process must be authorized by a user with the respective permission. A confirmation pop-up window appears for each change to give a clear overview of the changes to be made and to allow the user to comment on his actions (see Figure 3-4). The underlying user management functionality is used to assign permissions and to define security levels. Within the audit trail the three necessaries of the electronic signature are stored:

I. Reason/context
II. Timestamp
III. Printed user name

Actions that need to be authorized for running processes include:

- Starting/stopping of processes
- Changing values (e.g. setpoints)
- Acknowledging and clearing alarms
- Entering/altering of off-line data
- Entering data into programmed pop-up consoles
- Entering user comments
- Adding/altering descriptive context data (attributes)
- Configurational changes (e.g. alarm limits, data logging properties or port references).



EZC001	37.000 °C
EZC002	36.960 °C
EZC003	37.020 °C
EZC004	37.000 °C

Confirmation

Change Value of 'sp_DO'

Reactor: EZC004

Old: 30

New: 40

Reason

Securecell AG

•••••••••••••

OK Cancel

Port	Unit	EZC001	EZC002	EZC003	EZC004
17 CONTROL OUTPUT					
co_AirFlow		8.9679	4.6646	4.5907	4.6684
co_DO	[%]	30.176	29.303	30.718	29.515
co_FeedFlow	[%]	0	37.029	37.031	36.995
co_Stirrer	[%]	30.002	30.012	30.004	30.009
co_Temp	[%]	-0.075488	1.058	-0.44501	0.11491
co_pH	[%]	2.0783	-1.3233	-2.5617	1.5893
OFFLINE_SIM					

Figure 3.2: Example for electronic signature in Lucullus®. A clear action (Change Vale of 'sp_DO') the old and new value, a field for a specific reason and the username and password are required.

3.3 Audit Trail

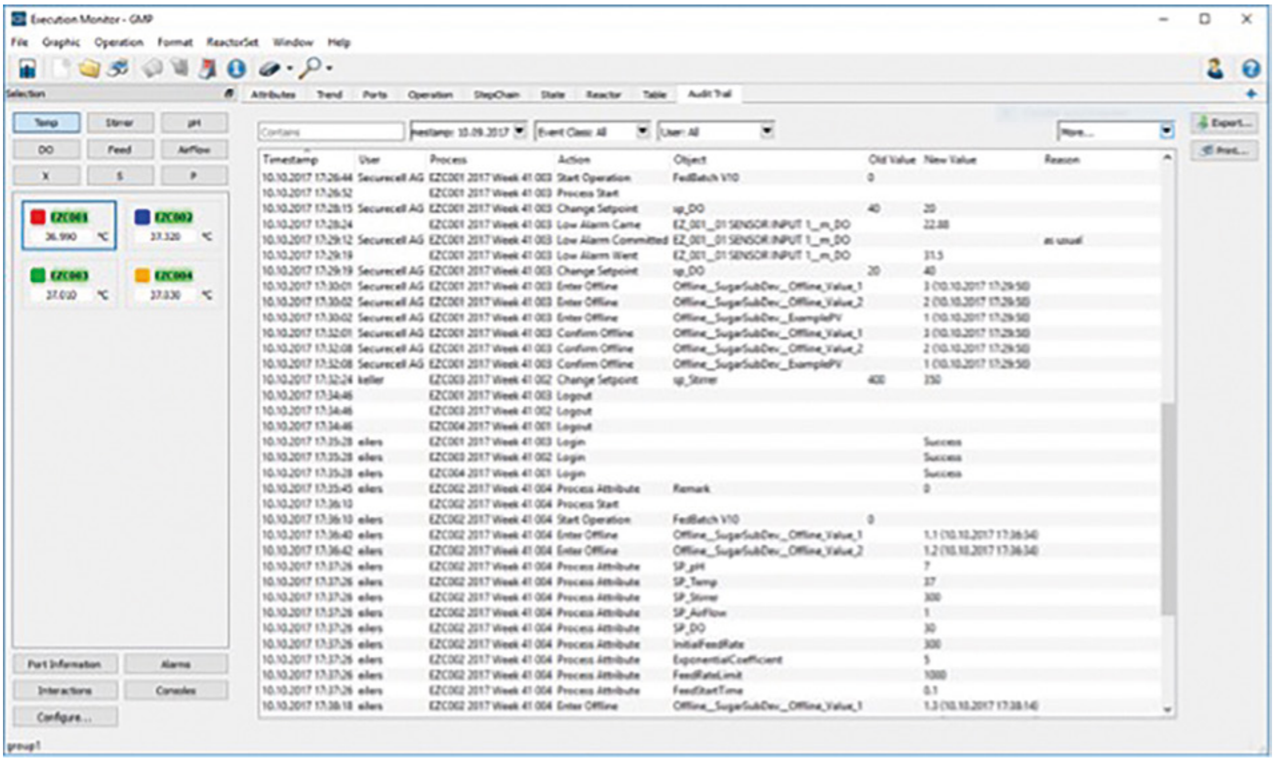
Lucullus® provides a continuous audit trail. The audit trail cannot be turned off and cannot be manipulated via the user interface. The audit trail is available in two parts.

The typical user-relevant audit trail is the process related audit trail, which logs all events in the context of specific processes. The logged events have the following information's:

Event time:	Date and time
Process Name:	Event-related process
Related User:	User ID if a user related event is logged,
Event type:	Login, start tool, start of the process, set/change value, alert, save, logout,...
Add. Information:	Old value, new value, reason,...

To facilitate inspection of these entries, it is possible to both export the table (see Figure 3-2) to common spreadsheet formats or directly print the table on a local printer. Additionally, extensive filter options enable efficient search for entries and allow condensed audit trail tables focusing on different activities. Together with the already available reporting functionality in Lucullus®, the software fully complies with the requirement to obtain clear printed copies of all electronically stored records.

The second audit trail acts on the database level. This allows traceability of all changes even in the system configuration itself. This second level cannot be accessed via the standard user interface to exclude manipulations.



Timestamp	User	Process	Action	Object	Old Value	New Value	Reason
10.10.2017 17:26:44	Securecell AG	EZC001 2017 Week 41 003	Start Operation	FedBatch V10	0		
10.10.2017 17:26:52		EZC001 2017 Week 41 003	Process Start				
10.10.2017 17:28:15	Securecell AG	EZC001 2017 Week 41 003	Change Setpoint	sp_DO	40	20	
10.10.2017 17:28:24		EZC001 2017 Week 41 003	Low Alarm Came	EZ_001__01 SENSOR INPUT 1__m_DO		22.88	
10.10.2017 17:29:12	Securecell AG	EZC001 2017 Week 41 003	Low Alarm Committed	EZ_001__01 SENSOR INPUT 1__m_DO			as usual
10.10.2017 17:29:19		EZC001 2017 Week 41 003	Low Alarm Went	EZ_001__01 SENSOR INPUT 1__m_DO		31.5	
10.10.2017 17:29:19	Securecell AG	EZC001 2017 Week 41 003	Change Setpoint	sp_DO	20	40	
10.10.2017 17:30:01	Securecell AG	EZC001 2017 Week 41 003	Enter Offline	Offline_SugarSubDev__Offline_Value_1		3 (10.10.2017 17:29:50)	
10.10.2017 17:30:02	Securecell AG	EZC001 2017 Week 41 003	Enter Offline	Offline_SugarSubDev__Offline_Value_2		2 (10.10.2017 17:29:50)	
10.10.2017 17:30:02	Securecell AG	EZC001 2017 Week 41 003	Enter Offline	Offline_SugarSubDev__ExamplePV		1 (10.10.2017 17:29:50)	
10.10.2017 17:32:01	Securecell AG	EZC001 2017 Week 41 003	Confirm Offline	Offline_SugarSubDev__Offline_Value_1		3 (10.10.2017 17:29:50)	
10.10.2017 17:32:08	Securecell AG	EZC001 2017 Week 41 003	Confirm Offline	Offline_SugarSubDev__Offline_Value_2		2 (10.10.2017 17:29:50)	
10.10.2017 17:32:08	Securecell AG	EZC001 2017 Week 41 003	Confirm Offline	Offline_SugarSubDev__ExamplePV		1 (10.10.2017 17:29:50)	
10.10.2017 17:32:24	keller	EZC003 2017 Week 41 002	Change Setpoint	sp_Stirrer	400	350	
10.10.2017 17:34:46		EZC001 2017 Week 41 003	Logout				
10.10.2017 17:34:46		EZC003 2017 Week 41 002	Logout				
10.10.2017 17:34:46		EZC004 2017 Week 41 001	Logout				
10.10.2017 17:35:28	eilers	EZC001 2017 Week 41 003	Login			Success	
10.10.2017 17:35:28	eilers	EZC003 2017 Week 41 002	Login			Success	
10.10.2017 17:35:28	eilers	EZC004 2017 Week 41 001	Login			Success	
10.10.2017 17:35:45	eilers	EZC002 2017 Week 41 004	Process Attribute	Remark		0	
10.10.2017 17:36:10		EZC002 2017 Week 41 004	Process Start				
10.10.2017 17:36:10	eilers	EZC002 2017 Week 41 004	Start Operation	FedBatch V10	0		
10.10.2017 17:36:40	eilers	EZC002 2017 Week 41 004	Enter Offline	Offline_SugarSubDev__Offline_Value_1		1.1 (10.10.2017 17:36:34)	
10.10.2017 17:36:42	eilers	EZC002 2017 Week 41 004	Enter Offline	Offline_SugarSubDev__Offline_Value_2		1.2 (10.10.2017 17:36:34)	
10.10.2017 17:37:26	eilers	EZC002 2017 Week 41 004	Process Attribute	SP_pH		7	
10.10.2017 17:37:26	eilers	EZC002 2017 Week 41 004	Process Attribute	SP_Temp		37	
10.10.2017 17:37:26	eilers	EZC002 2017 Week 41 004	Process Attribute	SP_Stirrer		300	
10.10.2017 17:37:26	eilers	EZC002 2017 Week 41 004	Process Attribute	SP_AirFlow		1	
10.10.2017 17:37:26	eilers	EZC002 2017 Week 41 004	Process Attribute	SP_DO		30	
10.10.2017 17:37:26	eilers	EZC002 2017 Week 41 004	Process Attribute	InitialFeedRate		300	
10.10.2017 17:37:26	eilers	EZC002 2017 Week 41 004	Process Attribute	ExponentialCoefficient		5	
10.10.2017 17:37:26	eilers	EZC002 2017 Week 41 004	Process Attribute	FeedRateLimit		1000	
10.10.2017 17:37:26	eilers	EZC002 2017 Week 41 004	Process Attribute	FeedStartTime		0.1	
10.10.2017 17:38:18	eilers	EZC002 2017 Week 41 004	Enter Offline	Offline_SugarSubDev__Offline_Value_1		1.3 (10.10.2017 17:38:14)	

Figure 3.3: Example of an audit trail with the information of timestamp, User, Process, Action, Object, Old Value, New Value and Reason.

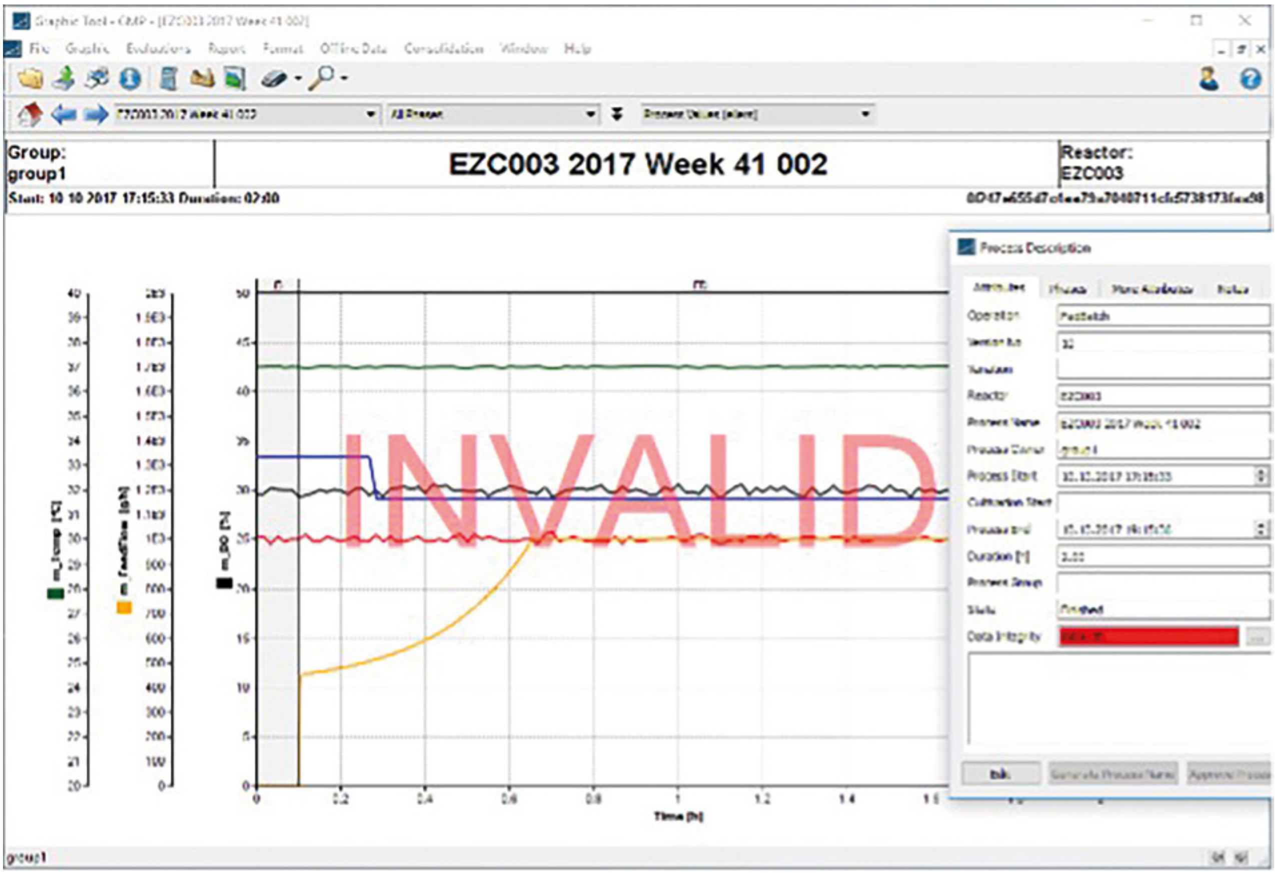
3.4 Archiving and Retrieval

The Lucullus® interface is designed to prevent any deletion of processes or any changes to the raw signals. Furthermore, resources like process control recipes (operations) or formats for tables or graphics cannot be deleted if they are linked to processes or reports in the database (data integrity checks). In addition to these measures taken on the user interface, the Lucullus Oracle® database has highly restricted accessibility database with password protection.

All data records are stored in a password protected database (Oracle). The customer is responsible to keep database passwords separate from application users. Nevertheless, Lucullus® offers the verification of data integrity by evaluating checksums at the database level. This function detects all signals that have been corrupted and thus possess invalid checksums. The deletion of whole processes, including all connected signals, would also be detected. There is a global data validity check for all processes in the database. In addition, invalidity will directly be detected when a process is loaded from the database and be prominently displayed. With the knowledge about the corrupt time series at hand, further investigations could reveal the type of manipulations made and the valid equivalent of the signal could be recovered from the database backups.

On the user interface level, Lucullus® allows users with the corresponding right to export data in various formats and prints. According to the visualization type the following formats are supported: .xlsx, .csv, .txt, .doc, .pdf, .png, .jpeg, .svg.

Graphs and tables created with a certain defined and saved format will be marked with a format-specific identifier code (hash code). In created reports, this identifier code can be used as a proof that the data is presented consistently, as changes made to the formats, such as different axis scaling, would result in a different identifier code.



Group:
group1

EZC003 2017 Week 41 002

Reactor:
EZC003

Start: 10 10 2017 17:15:33 Duration: 02:00

0D47a655d7c1ee79a7048711cfc5738173fea98

Operation	Fedbatch
Version No	32
Variation	
Reactor	EZC003
Process Name	EZC003 2017 Week 41 002
Process Owner	group1
Process Start	10.10.2017 17:15:33
Cultivation Start	
Process End	10.10.2017 19:15:33
Duration [h]	2.00
Process Group	
Status	Finished
Data Integrity	[illegible]

Figure 3.4: Example for a process which data was altered on the database level and that was therefore identified as invalid when loaded. The identifier code for consistent data representation can be seen below the reactor name in the top right corner

4 DETAILED EVALUATION OF LUCULLUS®

4.1 Controls for closed systems

PARAGRAPH / POINT	QUESTIONS / REQUIREMENT	COMMENTS
11.10 (a) Point 1	Is the system validated?	The client is responsible for the validation after an in-house installation and configuration. The validation should follow an established system life cycle methodology. Lucullus® is developed by Securecell AG and tested in-house. The validation of the application of Lucullus® can be supported by Securecell AG during projects upon requests.
11.10 (a) Point 2	Is there the ability to discern invalid or altered records?	Yes. This is ensured by multiple security checks. The first check is the Audit trail. The second verification of data integrity by evaluating checksums at the database level. This function detects all signals that have been corrupted and thus possess invalid checksums. The deletion of whole processes, including all connected signals, would also be detected. There is a global data validity check for all processes in the database. In addition, invalidity will directly be detected when a process is loaded from the database and be prominently displayed.
11.10 (b) Point 1	Is the system able to generate accurate and complete copies of electronic records on paper?	Yes. All process data and the audit trail can be displayed and printed directly from the software.
11.10 (b) Point 2	Is the system able to generate accurate and complete copies of records in electronic form for inspection, review and copying by the agency?	Yes. Both process data can be exported as .txt, .csv and .xlsx file as well as visualized in figures (.jpeg, png) and pdf. Audit trails, as well as process data, can be integrated into a report which can be saved and exported as a .pdf.
11.10 (c)	Are the records readily retrievable throughout their retention period?	Yes. The Graphic tool allows access to all recorded and imported data. Clients should also specify retention periods and define procedures for archiving, backup and retrieval of electronic records.
11.10 (d)	Is the system access limited to authorized individuals?	Yes With local user management, only authorized individuals can log on to the system using their user ID and password. Costumers should ensure that only individuals who have a legitimate reason to use the system should be granted physical access to the system (e. g. HMI devices, engineering system). As in requirement 11.10(g), it is generally interpreted to refer to both physical access and logical access.
11.10 (e) Point 1	Is there a secure, computer-generated, time-stamped audit trail available that records the date and time of operator entries and actions that create, modify, or delete electronic records?	Yes The audit trail is secure within the system and cannot be changed by a user. Changes during production can be traced back by the system itself and contain information with a time stamp, user ID, event type, old and new value and comment.
11.10 (e) Point 2	If a change is made to electronic data, is previously recorded information still available, i.e. not obscured by record changes?	Yes The old and new values are recorded in an audit trail. In addition, the time stamp and the user ID are recorded.
11.10 (e) Point 3	Is the audit trail of an electronic record retained throughout the entire retention period of the record?	Yes. The audit trail can be made available during the entire retention period. (see 11.10 (c))
11.10 (e) Point 4	Is the audit trail available for review and copying by the agency?	Yes. Availability is ensured by export of the audit trail as .pdf, .csv, .xlsx.
11.10 (f)	Are operational system checks used to enforce/ carry out permitted sequencing of steps and events?	Yes. The customer has the possibility to enforce/ carry out permitted sequencing of steps and events within the operation tool of Lucullus®.

11.10 (g)	Does the system ensure that only authorized individuals can use the system, electronically sign records, access the operation or the computer system input or output devices, alter a record, or perform other operations?	Yes. Lucullus® provides local user management with user groups, authorizations and users. It thereby regulates the administration of system access as well as individual authorizations. The use of an electronic signature requires password input.
11.10 (h)	Does the system determine the validity of the source of data input or operational instruction?	Yes There are several checks that are carried out. Operation Tool: Operational instructions are checked for their logical links. If a link is not possible, the operation is marked as not valid. Online Tool: If the data is not logged according to the driver configuration, a communication alarm will appear.
11.10 (i)	Does the system verify if a person who develops, maintains or uses electronic records or the electronic signature system has the education, training and experience to perform his assigned task?	Yes The Securecell AG offers either standard training courses or training related to client projects, which must be planned and executed separately. The costumer is responsible to plan these trainings and ensure attendance of the relevant persons.
11.10 (j)	Are written policies established and adhered to, that hold individuals accountable and responsible for actions initiated under their electronic signature?	Clients are responsible for implementing procedural controls.
11.10 (k) Point 1	Is an adequate control over the distribution of, access to and use of documentation for system operation and maintenance available?	Clients are responsible for providing procedural controls.
11.10 (k) Point 2	Is there a formal control procedure for revisions to system documentation that maintains a time-sequenced audit trail for those changes made by the pharmaceutical company?	Clients are responsible for providing procedural controls.

4.2 § 11.50 Signature manifestations

PARAGRAPH / POINT	QUESTIONS / REQUIREMENT	COMMENTS
11.50 (a) Point 1	Do the signed electronic records contain the printed name of the signer?	Yes Lucullus® allows to include a so-called "Displayed Name". The displayed name can be set up as a printed name by the customer.
11.50 (a) Point 2	Do the signed electronic records contain date and time when the signature was executed?	Yes Time and date are recorded.
11.50 (a) Point 3	Do the signed electronic records contain the meaning associated with the signature (e.g. review, approval, authorship etc.)?	Yes The associated information about why the signature was performed is recorded.
11.50 (b) Point 1	Is the information that is associated with the signature (as stated in 11.50) underlying the same controls as the electronic records?	Yes
11.50 (b) Point 2	Is the information that is associated with the signature (as stated in 11.50) included in the electronic record in any human-readable form (e.g. electronic display or printout)?	Yes Yes, the electronic signature can be displayed and exported for a printout or pdf (e.g. in a report).

4.3 § 11.70 Signature / record linking

PARAGRAPH / POINT	QUESTIONS / REQUIREMENT	COMMENTS
11.70	Does the system ensure that an electronic signature is linked to the respective electronic record in a way that the signature cannot be excised, copied, or otherwise transferred to falsify an electronic record? The linkage between electronic record and an electronic signature is saved in the protected Lucullus® database (see explanation in section 3.3). There are no means for the customer to alter such information and linkages. For exports in the electronic form (e.g. .pdf) 3rd party software can be used to electronically sign the documents and prevent further editing.	The linkage between electronic record and an electronic signature is saved in the protected Lucullus® database (see explanation in section 3.3). There are no means for the customer to alter such information and linkages. For exports in the electronic form (e.g. .pdf) 3rd party software can be used to electronically sign the documents and prevent further editing.

5 CONDITIONS OF VALIDITY

This document is valid only for selected versions of Lucullus® in together with an ongoing support contract. List of selected versions of Lucullus® is available on request directly from Securecell AG.