M. K. JUCHHEIM GmbH & Co

Paperless recorder LOGOSCREEN *es*

Declaration of Conformity 21 CFR Part 11

White Paper

Contents

Contents

1 General

1.1 Introduction

In the pharmaceutical and food industries, and related industrial sectors, there is a mandatory requirement for the recording of product manfacture.

In the past, recorders that used paper for recording were applied for the documentation of process data. For consumer protection, the parameter values that had been recorded on the paper were archived for decades, so that a seamless registration of the production and traceability in the event of deviations could be assured.

The introduction of paperless recording techniques has shifted the recording process from paper to paperless recorders.

For the purposes of orderly and unambiguously traceable recording of electronic process data, the American federal health authority, the

“Food & Drug Administration (FDA)”

passed the **21 CFR Part 11** (Code of Federal Regulations) in 1997.

This legal code defines the requirements for **Electronic Records** and **Electronic Signature**, in other words the paperless recording of production procedures and the use of an electronic signature that corresponds to a handwritten signature.

Fulfilling the requirements of 21 CFR Part 11 is now fundamental for the world-wide acceptance of products from the pharmaceutical and food industries.

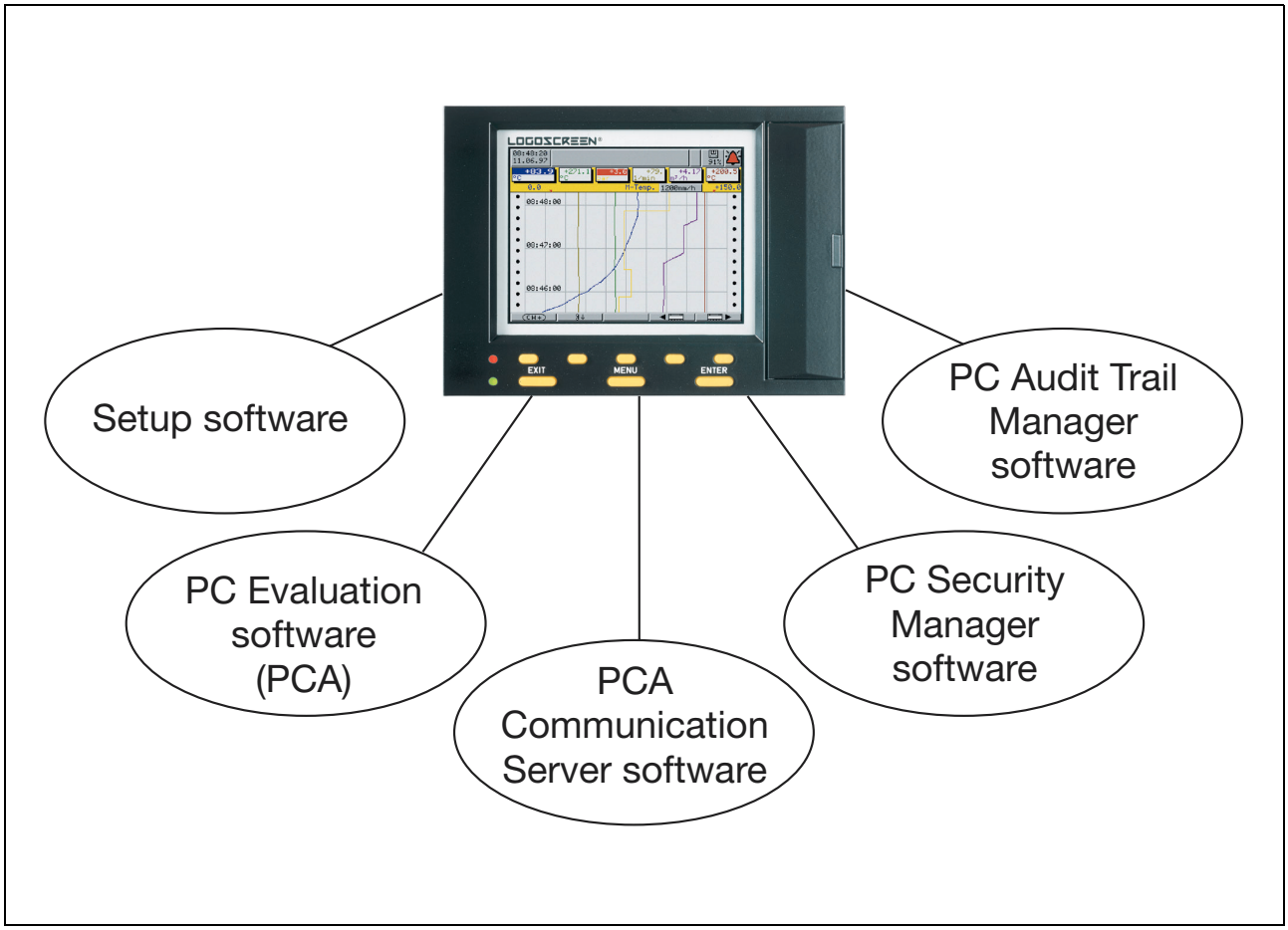
In Chapter 3, this “White Paper” provides the reader with statements on the measures for fulfillment of the requirements for every article of this part of the legal code.

1.2 Implementation of 21 CFR Part 11

The new paperless recorder **LOGOSCREEN *es*** from JUMO, together with its associated PC software components Setup, PCA, PCA Communication Server, Security Manager software and Audit Trail Manager software and their functionality fulfill the FDA requirements of 21 CFR Part 11 with respect to Electronic Records and Electronic Signature.

1.3 The system components of LOGOSCREEN *es*

The **LOGOSCREEN *es*** paperless recorder, together with its system components, forms a closed system in the sense of 21 CFR Part 11.



1.4 The PC software components

1.4.1 Setup software (to configure the recorder)

- dialog-led program for configuring the recorder,
- configuration data can be archived on data media and printed out

1.4.2 PC Evaluation software for process data (PCA)

- Visualization, archiving and evaluation of the stored data.

1.4.3 PCA Communication Server software (facilitates the reading out of data)

- can be used to retrieve data from the recorder via the serial interface,
- data retrieval can be performed manually or automatically, e.g. at 23.00 hrs every day,
- data can also be retrieved by remote access, using a modem.

1.4.4 PC Security Manager software (regulates the access to the system)

- manages the user list for the PC and the recorder,
- checks the access of users to the PC programs, and enables or refuses access to the system,
- ensures the authenticity of the electronic signature.

1.4.5 Recorder Security Manager software (regulates the access to the recorder)

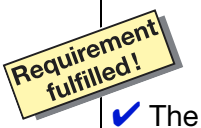
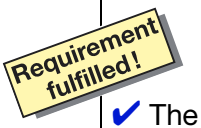
- stores the user list in the recorder,
- checks access to the recorder, and enables or refuses access,
- ensures the authenticity of the electronic signature.

1.4.6 PC Audit Trail Manager software (registers and stores all actions)

- registers operator actions with a time stamp, operator name, details, and reason for the alteration,
- stores and confirms all actions performed by the user.

2 Evaluation of the Requirements

The following comments are based on the assumption that the reader is already familiar with the fundamental requirements of 21 CFR Part 11.

Para.	Requirements: Subpart B: Electronic Records
§11.10 *Controls for closed systems*	
(a)	*Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.*  ✔ The system, consisting of the paperless recorder (hereinafter referred to as recorder) and the associated PC programs, is validated to ensure accuracy, reliability and consistent performance as intended. ✔ It is assured that invalid or altered documents (or attempts at tampering) are recognized, recorded in the audit trail, and are not available for evaluation.
(b)	*The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.*  ✔ All data are stored in a proprietary binary format that is unpublished and protected by a checksum algorithm. ✔ The process data are displayed on the recorder or PC in a readable form. ✔ The JUMO PC Evaluation software is provided for the display of the data on a PC, and all stored data can be visualized, copied or printed out with the aid of this software.
(c)	*Protection of records to enable their accurate and ready retrieval throughout the records retention period.*  ✔ The data are stored in the internal storage system of the computer. ✔ The internal storage system of the recorder is not used for data transfer. ✔ The data archived in the internal storage can be retrieved by authorized persons via a serial interface or to a compact flash-card, and then archived in the PC. ✔ Access to the serial interface is protected by a user ID and password. Flash-card access is mechanically locked and electronically monitored. ✔ Security against manipulation of the data is assured by using a proprietary binary format that is unpublished and protected by a checksum algorithm. ✔ The data that are available on the flash-card are stored on a PC system for the purposes of archiving and evaluation.

2 Evaluation of the Requirements

Para.	Requirements: Subpart B: Electronic Records
§11.10 ***Controls for closed systems***	
(d)	*Limiting system access to authorized individuals.* Requirement fulfilled! ✔ Access to the system is limited by assigning individually defined rights to authorized individuals. ✔ Every user must log on to the system by using a user ID and a password. ✔ The access rights are assigned by the administrator, and every access to the system is checked by the Security Manager software. ✔ Only the administrator has the power to alter the access rights of users. ✔ Data that are already registered and archived are not altered by a change to access rights.
(e)	*Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.* Requirement fulfilled! ✔ The Audit Trail software is an integral components of the instrument software and the associated PC programs (separate audit trails). The audit trail is generated automatically, and can not be configured or switched off. ✔ It is assured that all actions that are initiated by operating personnel are automatically registered and archived, together with the date and time. ✔ Audit trail data cannot be altered or deleted in the instrument. ✔ The addition of texts or comments is only possible for authorized persons, after entering the user ID and the password. ✔ All data that are stored in the audit trail of the recorder are copied over to the JUMO-PC Evaluation software, together with the process data, and are available via this software. ✔ Audit trail data can be made accessible for purposes of checking at any time, using the PC Evaluation software.
(f)	*Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.* Requirement fulfilled! ✔ The sequence of steps, such as for batch recording, is fixed. So it is possible to select by configuration whether a batch record requires an electronic signature or not. If a signature is required, it will, for instance, not be permitted for batch records in progress (as opposed to batch records that are finished). ✔ Another situation: the recorder can be so configured that the user, when logging off, is requested to provide an electronic signature for the time for which he or she was responsible (i.e. logged on).

2 Evaluation of the Requirements

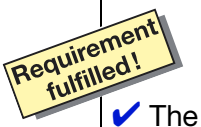
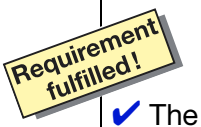
Para.	Requirements: Subpart B: Electronic Records
§11.10 *Controls for closed systems*	
(g)	*Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.* Requirement fulfilled! ✔ Access rights to the system are assigned by the administrator. ✔ These access rights are checked by the Security Manager software in the recorder, and checked and managed by the PC Security Manager software. ✔ Only persons with “Administrator rights” can set up or delete user lists. ✔ Logging on with a unique identification (user ID and password) is always a precondition for a user to gain access to the system. ✔ A time limitation for the usability of a password can be fixed by the administrator. When this time has expired, the user must enter a new password, otherwise the access rights will be lost.
(h)	*Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.* Requirement fulfilled! ✔ The recorder can only be configured or operated by persons who are authorized to do so. This also applies to the connection of sensor leads or interfaces to the locked back panel of the recorder. ✔ Data that are stored in the recorder are automatically linked with a unique and eternally valid, unambiguous instrument ID number (production number), so that they can be unambiguously assigned.
(i)	*Determination that persons who develop, maintain, or use electronic record / electronic signature systems have the education, training, and experience to perform their assigned tasks.* Requirement fulfilled! ✔ All persons participating in the development of the LOGOSCREEN *es* and the associated PC software were trained in the contents and requirements of 21 CFR Part 11. ✔ Appropriate training courses will also be offered for users of the LOGOSCREEN *es*.
(j)	*The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.* Not applicable! This is the responsibility of the user.

2 Evaluation of the Requirements

Para.	Requirements: Subpart B: Electronic Records
§11.10 *Controls for closed systems*	
(k)	*Use of appropriate controls over systems documentation including:* *(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.* *(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.* Not applicable! This is the responsibility of the user.

Para.	Requirements: Subpart B: Electronic Records
§11.30 *Controls for open systems*	
	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality. Not applicable! The LOGOSCREEN *es* and the associated PC programs represent a closed system.

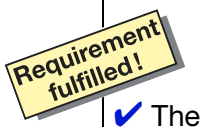
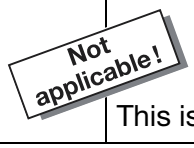
2 Evaluation of the Requirements

Para.	Requirements: Subpart B: Electronic Records
§11.50 *Signature manifestations*	
(a)	*Signed electronic records shall contain information associated with the signing that clearly indicates of the following:* *(1) The printed name of the signer;* *(2) The date and time when the signature was executed; and* *(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.*  ✔ The electronic signature that is assigned to the relevant records is presented in a readable form on the recorder or by the PC Evaluation software. In every case, the electronic signature includes the name of the signer in block capitals, the date and time (to the second) when the signature was created, as well as the meaning of the signature. Batches, time periods and comments can all be linked to electronic signatures. Manipulation is not possible, since the recorder and the associated PC programs generate the time information themselves. An alteration of the clock setting on the recorders requires that the user is authorized to do so. Every alteration is registered in an unerasable fashion in the audit trail.
(b)	*The items identified in paragraphs (a)(1), (a)(2) and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).*  ✔ The electronic signature is an integral part of the raw data of the recorder. ✔ The raw data of the recorder consist of the electronic record, the electronic signature, audit trail data, and the checksum. The format is generated in the recorder, and is used in unalterable form for the transfer of data to and storage in the PC. ✔ The raw data of the recorder, including the electronic signature, are recorded in a proprietary binary format that is unpublished and protected by a checksum algorithm. The raw data of the recorder, including the electronic signatures that are unerasably linked to them, are proof against manipulation. ✔ The electronic signature is attached to the readable version (display or printout) of the electronic document that is derived from the raw data of the recorder. ✔ The printout or the electronic form of the printable document (PDF format) is marked with a notice that it is presented in a form derived from the raw data of the recorder.

2 Evaluation of the Requirements

Para.	***Requirements:*** ***Subpart B: Electronic Records***
§11.70 ***Signature/record linking***	
	Electronic signatures and handwritten signatures executed to electronic records 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. Requirement fulfilled! ✔ The raw data of the recorder, including the electronic signature, are recorded in a proprietary binary format that is unpublished and protected by a checksum algorithm. ✔ The raw data of the recorder, including the electronic signatures that are unerasably linked to them, are proof against manipulation. ✔ The Security Manager software functions are set up on the recorder and in the associated PC programs in an unalterable fashion, with the following tasks: PC Security Manager software: - creates and manages the user list for the PC and the recorder - checks access to the PC programs, and enables access - ensures the authenticity of the electronic signature Security Manager software (recorder): - stores the user list in the recorder - checks access to the recorder, and enables access - ensures the authenticity of the electronic signature ✔ The defined access to the recorder or the associated PC programs via the Security Manager software excludes the falsification or copying of an electronic signature by an individual. ✔ The recorder and the associated PC programs do not permit alteration or removal of the electronic signature. The recorder and the associated PC programs detect any attempt at alteration or removal of an electronic signature, and indicate this attempt. ✔ The event is registered in an unerasable fashion in the audit trail.

2 Evaluation of the Requirements

Para.	Requirements: Subpart B: Electronic Records
§11.100 ***General requirements***	
(a)	*Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.*  ✔ The PC Security Manager software is used by the administrator to set up the users for the recorder, their rights, their initial passwords and password restrictions, and to transfer them to the recorder, collected in a user list and encoded. ✔ The PC Security Manager software ensures that the combination of user name and user ID is unique and unambiguous for every user who is registered in the user list. ✔ Users can be barred from exercising rights (by the administrator), but the users cannot be removed from the user list. ✔ The Security Manager software of the recorder is based on the user list, and thus takes care of the authenticity of the electronic signature.
(b)	*Before an organization establishes, assigns, certifies, or otherwise sanctions an in individual's electronic signature or any element of such signature, the organization shall verify the identity of the individual.*  This is the responsibility of the owner of the system.
(c)	*Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.*  This is the responsibility of the owner of the system.
(1)	*The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.*  This is the responsibility of the owner of the system.
(2)	*Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.*  This is the responsibility of the owner of the system.

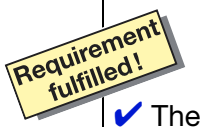
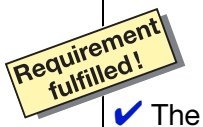
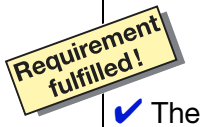
2 Evaluation of the Requirements

Para.	Requirements: Subpart B: Electronic Records
§11.200 *Electronic signature components and controls*	
(a) (1)	*Electronic signatures that are not based upon biometrics shall:* *Employ at least two distinct identification components such as an identification code and password.* Requirement fulfilled! ✔ The electronic signature can only be executed by a user who has been authorized (by the administrator), and who has been authenticated by the access control system (Security Manager software) of the recorder or the associated PC programs, by means of the user ID (user name) and the password.
(i)	*When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.* Requirement fulfilled! ✔ Only one user at a time can be authorized by the Security Manager on the recorder or the PC Security Manager, to the extent of the rights assigned to him (by the administrator). ✔ An electronic signature can only be executed by the user who is logged on via the recorder or the associated PC programs. The user is compelled on the first and on every subsequent occasion to undergo complete authentication by the Security Manager software, by means of the user ID (user name) and password. ✔ Before executing the electronic signature, the user is informed of the following situation by a text message that reads: “Your signature is legally binding and is equivalent to your handwritten signature!”
(ii)	*When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.* Requirement fulfilled! ✔ An electronic signature can only be executed by the user who has been authenticated by the recorder or the associated PC programs. The user is compelled on the first and on every subsequent occasion to undergo complete authorization by the Security Manager software, by means of the user ID (user name) and password.

2 Evaluation of the Requirements

Para.	Requirements: Subpart B: Electronic Records
§11.200 *Electronic signature components and controls*	
(2) (3)	*Be used only by their genuine owners; and be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.* Requirement fulfilled! ✔ This is ensured by the procedure laid down for the creation and management of the user list, which forms the basis for the authorization and authentication of a user. ✔ It is not possible for a single user, acting alone, to use any other electronic signature but his own. ✔ Any such attempt will be detected and registered in an unerasable fashion in the audit trail. ✔ Every user makes use of a password that is set up in accordance with the established restrictions. This password is known only to the user. No one can read out passwords from the recorder, not even with the aid of the PC programs.
(b)	*Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.* Not applicable! No electronic signature based on biometrics is envisaged.

Para.	Requirements: Subpart B: Electronic Records
§11.300 *Controls for identification codes/passwords*	
(a)	*Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:* *Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.* Requirement fulfilled! ✔ The PC Security Manager software is used by the administrator to set up the users for the recorder, their rights and password restrictions, and to transfer them to the recorder, collected in a user list and encoded. ✔ The assignment of all the data to a recorder is ensured by a unique and eternally valid, unambiguous instrument ID number (production number). ✔ The PC Security Manager software and the Security Manager software of the recorder ensure the uniqueness of each combination of user ID and password.

Para.	Requirements: Subpart B: Electronic Records
§11.300 *Controls for identification codes/passwords*	
(b)	*Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).*  ✔ The user list is the foundation for the control of access to the recorder and the PC. The same high level of security criteria is applied here as for the electronic records. ✔ Manipulation of the user list will be detected. In such a case the use of this user list will be barred and the event is registered in an unerasable fashion in the audit trail. ✔ The Security Manager software of the recorder and the PC Security Manager software ensure that there is a check of the restrictions set up by the administrator, including obsolescence of passwords, at every alteration of the user list or check of the access control. ✔ A user whose password is out of date is barred from the system, and the event is registered in an unerasable fashion in the audit trail. Only the administrator can re-enable access for this user.
(c)	*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.*  ✔ The recorders and the associated PC programs do not use marks, tokens, or the like. Security is provided by the user rights and password restrictions that are set up by the administrator. For instance, the administrator can set up an initial password that must be altered by the user immediately on the occasion of first access, so that this new password is known only to the user. The duration of the validity of the password can also be defined. ✔ Failure to observe the restrictions leads to withdrawal of the user rights. ✔ The event is registered in an unerasable fashion in the audit trail.
(d)	*Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.*  ✔ The PC Security Manager software and the Security Manager software of the recorders prevent unauthorized access. Any such attempt is detected and registered in an unerasable fashion in the audit trail of the recorder or the audit trail of the PC.

2 Evaluation of the Requirements

Para.	Requirements: Subpart B: Electronic Records
§11.300 ***Controls for identification codes/passwords***	
(e)	*Initial and periodic testing of devices, such as tokens or 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.* Not applicable! The recorders and the associated PC software do not use or generate marks, tokens, or other such devices that bear user identification code or password information.

3 Literature references

[1] Mass & Peither GMP Verlag
21 CFR 210/211 cGMP FOR FINISHED PHARMACEUTICALS
incl. 21 CFR 11 electr. Records/electr. Signature

M. K. JUCHHEIM GmbH & Co

Street address:
Moltkestraße 13 - 31
36039 Fulda, Germany
Delivery address:
Mackenrodtstraße 14
36039 Fulda, Germany
Postal address:
36035 Fulda, Germany
Phone: +49 661 6003-0
Fax: +49 661 6003-607
E-mail: mail@jumo.net
Internet: www.jumo.net

JUMO Instrument Co. Ltd.

JUMO House
Temple Bank, Riverway
Harlow, Essex CM20 2TT, UK
Phone: +44 1279 635533
Fax: +44 1279 635262
E-mail: sales@jumo.co.uk
Internet: www.jumo.co.uk

JUMO PROCESS CONTROL INC.

885 Fox Chase, Suite 103
Coatesville, PA 19320, USA
Phone: 610-380-8002
1-800-554-JUMO
Fax: 610-380-8009
E-mail: info@JumoUSA.com
Internet: www.JumoUSA.com

09.02/00409194