INFORMATION

No. **INF02/70 Issue 3** Date: **October 2007** Product **SM1000 and SM2000 Videographic Recorders**
Manuals **IM/SM1000 and IM/SM2000**

Guidance on the use of the SM1000 and SM2000 Videographic Recorders for Electronic Record Keeping in FDA Approved Processes

Introduction

On August 20th 1997 the Food and Drug Administration made 21 CFR Part 11 effective. This regulation is summarized as follows:

'The Food and Drug Administration (FDA) is issuing regulations that provide criteria for acceptance by FDA, under certain circumstances, of electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper. These regulations, which apply to all FDA program areas, are intended to permit the widest possible use of electronic technology, compatible with FDA's responsibility to promote and protect public health. The use of electronic records as well as their submission to FDA is voluntary.'

This guide provides details of the relevant sections of 21 CFR Part 11 and gives information on how the SM1000 and SM2000 Videographic Recorders can be used to meet these FDA requirements for the creation of electronic records in a closed system.

FDA 21 CFR Part 11 Subpart B – Electronic Records, Section 11.10: Controls for Closed Systems

'Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity and, when appropriate, the confidentiality of electronic records and ensure that the signer cannot repudiate the signed record as not genuine.'

Process data can be archived in either a) Text Format or b) Binary Format:

a) Text Format
All process data recorded by the SM1000 and SM2000 is protected by an encrypted 'digital signature'. Via the use of DataManager data review software this 'digital signature' can be checked to validate the integrity of the data. If any part of the data record is changed the DataManager software warns the user of the invalid nature of the record.

b) Binary Format
Process data can be archived in a binary encoded format which can be viewed only in a human-readable form through the use of ABB's DataManager review software. The recorded data contains built-in data integrity checks for each block of data (maximum of 240 samples per block) in order to detect any corruption or attempted falsification of the record. The DataManager software checks the data against the built-in checksums to validate the integrity of the data and to warn the user of any invalid records

FDA 21 CFR Part 11 Section 11.10 (a)

'Validation of systems to ensure accuracy, reliability, consistent intended performance and the ability to discern invalid or altered records.'

Validation is a function usually performed by the end-user or a third party acting on behalf of the end-user. The SM1000 and SM2000 have been developed (including the design of the recorder's software) and manufactured in ISO9001:1994 standard processes. Further details on the manufacturing and design practices applied to the SM1000 and SM2000 can be provided by ABB to assist the customer with the validation of the Videographic Recorders. The accuracy of the recorder measurements can be ensured by exercising the system calibration procedures described in the relevant User Guide. The SM1000 and SM2000 have an encoded audit log feature which allows the identification of changes to the system by recording the nature, time/date and authorized user of the modification.

FDA 21 CFR Part 11 Section 11.10 (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 (FDA).'

The SM1000 and SM2000 can create process data files on Compact Flash (CF) cards. These data files are created from secure records stored in internal flash memory. Error detection algorithms are employed to ensure that the stored data faithfully represents the actual raw measurements made by the recorder. Each write to the archive media is also verified to ensure the integrity of the data record. The archived process data files can be viewed using the DataManager review software. The data can be viewed and printed in tabular or graphical formats. Standard spreadsheet formats (e.g. Microsoft Excel) of the archived data files can be created for viewing by users who do not have the DataManager software.

FDA 21 CFR Part 11 Section11.10 (c)

'Protection of records to enable their accurate and ready retrieval throughout the records retention period.'

The SM1000 and SM2000 use solid-state flash memory, in the form of Compact Flash (CF) cards, for data storage. Data retention for these devices is specified as a minimum of 10 years. They provide zeropower data retention, i.e. the data integrity is not dependent on battery back-up. The data is not affected by magnetic fields. For even longer-term data storage the archive files can be copied to CDROM or to a network file server.

FDA 21 CFR Part 11 Section11.10 (d)

'Limiting system access to authorized individuals.'

The SM1000 and SM2000 provide the ability to limit access to the instruments configuration and critical operator functions. Two different security modes can be configured in the instruments:

1) Password Protection
Up to 12 users, each with a unique ID and password, can be created to control access to critical operator functions and configuration parameters.

The ID can be alphanumeric and up to 20 characters in length.

The passwords can be alphanumeric and the minimum number of characters allowable in a password can be set from 4 to 20 characters.

To prevent password ageing a password expiry time can be set.

To prevent illegal use of user ID's a user can be de-activated after a configurable number of repeated wrong password entries.

Users can be de-activated after a configurable period (7 days to 1 year) of inactivity.

Different access privileges can be set for each user.

One of four levels of configuration access can be assigned to a user:

1) No access
2) The ability to load existing configuration files only
3) Limited access (read access plus the ability to adjust alarm trip values
4) Full read/write access

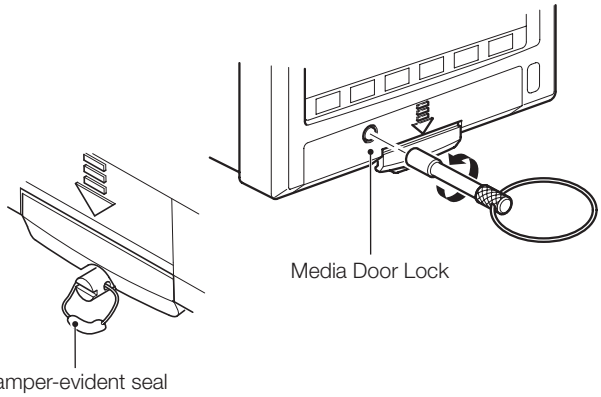
In order to gain access to the configuration or critical operator parameters a valid operator ID and password combination must be entered. The recorders do not have a secret override password.

Any modification of the instruments' configuration is recorded in the audit log identifying the user responsible for the change.

2) Security Switch Protection

Access to the instruments' configuration is protected by a physical internal switch. In order to gain access to the internal security switch it is necessary to remove the instrument from its case. A tamper-evident seal can be fitted to the securing screw to prevent the removal of the instrument from its case without breaking the seal.

In addition to these protection methods, access to the archive media [i.e. Compact Flash (CF) card] can be protected by a mechanical lock, fitted as standard on all units to the door on the front of the instrument.



Instrument Security

FDA 21 CFR Part 11 Section11.10 (e)

'Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator actions that create, modify or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained at least as long as that required for the subject electronic records and shall be available for agency review and copying.'

The SM1000 and SM2000 automatically produce a time-stamped audit trail that includes disk insertion and removal, power failure and recovery, configuration changes, file deletions, system diagnostics and calibration changes. This information is stored in an audit log which can be automatically archived to a permanent file on a Compact Flash (CF) card. A separate alarm/event log automatically produces a time-stamped record of all alarm state changes and can also be automatically archived to a permanent file. Each time the configuration of the recorder is changed a new file is created which can be stored as a permanent file to Compact Flash (CF) card. Each file is time-stamped to indicate the date and time when the change occurred. This allows the configuration at a previous time in a recorder's history to be maintained and for the configuration before and after a change to be reviewed.

The audit and alarm/event logs can be stored in an encoded format with checksum protection to prevent the falsification of its contents.

FDA 21 CFR Part 11 Section 11.10 (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.'

The recorders' security system outlined in part d) limits access to the system to modify any configuration parameters.

FDA 21 CFR Part 11 Section 11.10 (h)

'Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.'

The analog inputs provided on the SM1000 and SM2000 have built-in broken-sensor, and over- and under-range detection. Indication of these conditions is provided on the recorder's display and in the data files.

FDA 21 CFR Part 11 Section 11.10 (i)

'Determination that the persons who develop, maintain or use electronic record/electronic signature systems have the education, training and experience to perform their assigned tasks.'

Only suitably qualified people are employed in product design & development and their training is updated to meet advances in technology. Levels of competence and training needs are externally audited by the British Standards Institute (BSI) for our ISO9001 quality management system.

FDA 21 CFR Part 11 Section 11.10 (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.'

A design control system is used which is fully documented and traceable. This is externally audited by the British Standards Institute (BSI) for our ISO9001 quality management system. Documentation is provided for installation, configuration and operation in the instruments' User Guides.

FDA 21 CFR Part 11 Subpart B – Electronic Records, Section 11.50: Signature manifestations

a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

1) The printed name of the signer

2) The date and time when the signature was executed

3) The meaning (such as review, approval, responsibility or authorship) associated with the signature.

b) The items identified in paragraphs a) 1), a) 2), and a) 3) of this section shall be included as part of any humanreadable form of the electronic record (such as electronic display or printout).

The SM1000 and SM2000 electronic signatures are recorded with the operators username (up to 20 characters), the date and time at which the signature was activated and a 20-character message which the operator can use to indicate the purpose of the signature.

FDA 21 CFR Part 11 Subpart B – Electronic Records, Section 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.

Electronic signatures are stored in the SM1000 and SM2000 alarm/ event logs. This log can be stored to archive media in an encoded format with checksum protection to prevent the falsification of its contents. The archived alarm/event log and channel data files both contain the instrument tag and unique instrument serial number. This can be used to ensure that the electronic signature and the associated data are securely linked.

FDA 21 CFR Part 11 Subpart C – Electronic Signatures, Section 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 SM1000 and SM2000 do not allow the same username to be used by more than one operator. This function together with procedural controls can be used to meet this requirement.

FDA 21 CFR Part 11 Subpart C – Electronic Signatures, Section 11.200: Electronic signature components and controls.

a) Electronic signatures that are not based upon biometrics shall:

1) Employ at least two distinct identification components such as an identification code and 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 signature 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.

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.

2) Be used only by their genuine owners; and

3) 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.

To perform any electronic signing the SM1000 and SM2000 require the operator to provide a valid username and password. The SM1000 and SM2000 do not have security override codes. The security can only be overridden by the use of an internal switch, access to which can be protected by a tamper-evident seal.

FDA 21 CFR Part 11 Subpart C – Electronic Signatures, Section 11.300: Controls for identification codes/passwords.

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity.

The passwords can be alphanumeric and the minimum number of characters allowable in a password can be set from 4 to 20 characters. To prevent password ageing a password expiry time can be set. To prevent illegal use of user ID's a user can be de-activated after a configurable number of repeated wrong password entries. Users can be de-activated after a configurable period (7 days to 1 year) of inactivity.

FDA 21 CFR Part 11 Section 11.300 (a)

Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

The SM1000 and SM2000 do not allow the same username to be used by more than one operator.

FDA 21 CFR Part 11 Section 11.300 (b)

Ensuring that identification code and password issuances are periodically checked, recalled or revised (e.g., to cover such events as password ageing).

To prevent password ageing a password expiry time can be set. To prevent illegal use of user ID's a user can be deactivated after a configurable number of repeated wrong password entries. Users can be de-activated after a configurable period (7 days to 1 year) of inactivity. These features together with procedural controls can be used to meet these requirements.

Summary

ABB is an established world force in the design and manufacture of instrumentation. The quality, accuracy and performance of the Company's products result from over 100 years experience. The products are manufactured and designed using ISO9000 approved processes.

The SM1000 and SM2000 have been designed to meet the standards set out in 21 CFR part 11 and properly implemented they can be used as part of a validated system.

1a. All process data can be recorded in a binary encoded, tamper-proof format. The recorded data is further protected by error detection checks to ensure the authenticity of these records.

1b. Or all process data can be recorded in a text format that is protected by an encrypted 'digital signature' to ensure the authenticity of these records.

2. Solid state flash memory that is not reliant on battery back-up and which is not subject to magnetic fields is used to provide secure storage of data .

3. DataManager review software provides the ability to view the data records and audit trails in a human-readable form.

4. Password and physical security systems are provided in the recorders to limit access to authorized personnel. Provision is made to counter password ageing and attempted unauthorized access.

5. A detailed audit log accompanies all process data recorded by an SM1000 or SM2000. All system events including configuration changes, memory card removal/insertions, power failures and instrument calibrations are logged. All entries are time and date-stamped and include an operator ID where applicable. This log can be encoded and protected by built-in error checks to prevent/detect tampering or data corruption.

ABB has Sales & Customer Support expertise in over 100 countries worldwide

www.abb.com

Printed in UK (10.07)

INF02/70 Issue 3

ABB Limited
Howard Road, St Neots
Cambridgeshire
PE19 8EU
UK
Tel: +44 (0)1480 475321
Fax: +44 (0)1480 217948

ABB Inc.
125 E. County Line Road
Warminster
PA 18974
USA
Tel: +1 215 674 6000
Fax: +1 215 674 7183