FREQUENTLY ASKED QUESTIONS

Syngistix for AA and ICP-OES Enhanced Security Software: Compliance with 21 CFR Part 11 Regulations

The regulations of 21 CFR Part 11 (Title 21 – Food and Drugs of the Code of Federal Regulations) cover overall system compliance and include administrative, procedural and technical elements. Software alone cannot be compliant without the development and implementation of the other elements. Syngistix™ Enhanced Security™ (ES) Software for AA and ICP provides features that, when coupled with appropriate policies and procedure, fulfill the requirements for closed system electronic records in 21 CFR Part 11.

21 CFR Part 11 Subpart B – Electronic Records

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 to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

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

Q **Is it possible to see on the system whether or not records have been altered?**

A Syngistix ES software appends a check sum to all files and database records. Attempting to open a file that has been altered outside the system will generate an error message and an entry in the master event log. Records in the results database can be checked using the Check Signatures command in the Data Manager.

Q **Does the supplier have a quality management system?**

A Yes, PerkinElmer follows ISO 9001 standards.

Q **Can the system identify invalid records?**

A Syngistix ES software appends a check sum to all files or database records. Attempting to open a file that has been altered outside the system will generate an error message and an entry in the master event log.

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. 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.

Q **Is the system capable of producing accurate and complete copies of records in electronic form for inspection, review and copying by the FDA?**

A All files and data objects can be read using the Syngistix application and inspected using the included tools. In addition, most data objects can be exported as Text which can be viewed using a Text editor.

Methods

There is a Save As Text option for methods which will create a Text file.

Sample Information Files

Sample information files are always Text.

PerkinElmer®
For the Better

Results Database
Results database records can be examined using Access except for the OLE fields (copy of method, IEC or MSF models used to perform the analyses, and raw analytical data). Raw analytical data can be exported to a comma-delimited Text file using the application. Methods, IEC factors, and MSF files can be imported back into the application and be viewed, exported, or saved like the separate files.

IEC Files (ICP only)
IEC files can be opened by the application and saved as a Text file.

MSF Files (ICP only)
MSF files can be opened by the application and viewed using the MSF Viewer/Editor.

Wavelength Calibration Table (ICP only)
The Wavelength Calibration table (offset.tbl) is a Text file.

Dark Current Offset Table (ICP only)
The dark current offset table (DCSB.cal) is a Text file.

Audit Logs
The Master Event Log and the File Difference Log can be exported as Text using the appropriate viewer in the Data Manager.

Q **Is the system capable of producing accurate and complete copies of records in paper form for inspection, review and copying by the FDA?**

A **Methods**
Methods can be printed using the Print Active Window command when the Method Editor is the active window.

Sample Information Files
Sample information files can be printed using the Print Active Window command when the Sample Information Editor is the active window.

Results Database
Many records in the results database can be printed using various tools in the main Syngistix application or as reports from the Data Manager. Also, most records can be exported as comma-delimited Text which can be printed. Finally, most fields can be printed as reports directly using the Access database program.

IEC Files (ICP only)
IEC files can be printed using the Print Active Window command when the IEC Model Builder is the active window.

MSF Files (ICP only)
MSF files can be viewed using the MSF Viewer/Editor in the application. Copies of the model can be printed using a third party screen capture utility.

Wavelength Calibration Table (ICP only)
The Wavelength Calibration table (offset.tbl) is a Text file which can be printed using an Text editor.

Dark Current Offset Table (ICP only)
The dark current offset table (DCSB.cal) is a Text file which can be printed using a Text editor.

Audit Logs
The Master Event Log and the File Difference Log can be printed using the appropriate viewers in the Data Manager.

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

Q **Are the records readily retrievable throughout their retention period?**

A Records are always retrievable using the version of Syngistix ES software used to create them. Most files and database records are either in a Text format or can be exported to a Text format which can be retrieved for viewing using any Text editor. Also, the results database is an Access database which can be retrieved using Microsoft Access.

11.10 d Limiting system access to authorized individuals.

Q **Is system access limited to authorized individuals?**

A Syngistix and the computer that it runs on meet the requirements of a closed system.

Syngistix supports the Windows® log-in (password) and group assignments. Different Windows® groups can be assigned different Syngistix privileges consistent with their training. Groups of users can be assigned to different directory locations with access determined by settings in the Windows® operating system.

11.10 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.

Q **Is there a secure, computer generated, time stamped audit trail that records the date and time of operator entries and actions that create, modify, or delete electronic records?**

A The Master Event Log (audit trail) created by the system records every significant action performed by the operator which affects the analytical results or electronic records written to a file or database. A File Change Log monitors file or data set names and versions. Data set or file change data are included in each new version.

Each Master Event or File Change Log entry includes date, time, operator name, action performed, and other parameters which may be needed to describe what was done.

Check sums are applied to the Master Audit and File Change logs to detect any unauthorized changes. The logs are saved in a password-protected Access database.

Q **Upon making a change to an electronic record, is previously recorded information still available (i.e. not obscured by the change)?**

A The old version of any file or data set is copied to an History directory or, in the case of Methods, to an History database before the new version is saved. The version number of the file or data set is incremented to indicate that a changed version was created.

Once analytical data have been collected, no changes can be made to them in the Results database.

Q **Is an electronic record's audit trail retrievable throughout the record's retention period?**

A The Master Event Log or File Change Log can be retrieved at any time using the version of the Syngistix application used to create the record. The logs (audit trails) can also be exported as comma-delimited Text, which can be viewed using a Text editor or a spreadsheet program.

Q **Is the audit trail available for review and copying by the FDA?**

A The Master Event Log or File Change Log (audit trails) can be exported as comma-delimited Text, which can be copied and viewed using a Text editor or a spreadsheet program.

11.10 f Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

Q **If the sequence of system steps or events is important, is this enforced by the system (e.g. as would be the case in a process control system)?**

A Syngistix ES software performs a large number of method and analysis checks to ensure that all settings are valid before analyses are performed. Other analytical problems are flagged using messages in the results display window and on the printed log. Wizards are used to walk the user through particularly confusing tasks.

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.

Q **Does the system ensure that only authorized individuals can use the system, electronically sign records, access the operation or computer system input or output device, alter a record, or perform other operations?**

A Syngistix ES software and the computer that it runs on meet the requirements of a closed system.

Syngistix supports the Windows® log-in (password) and group assignments.

Different Windows® groups can be assigned different Syngistix privileges consistent with their training.

Groups of users can be assigned to different directory locations with access determined by settings in the Windows® operating system.

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.

Q **If it is a requirement of the system that input data or instructions can only come from certain input devices (e.g. terminals) does the system check the validity of the source of any data or instructions received?**

(Note: This applies where data or instructions can come from more than one device, and therefore the system must verify the integrity of its source, such as a network of weigh scales, or remote, radio controlled terminals).

A Syngistix ES software is always configured for a single spectrometer. The spectrometer serial number is recorded as part of the data records saved in the results database. User input can only come from the logged-in user.

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.

Q **Is the distribution of, access to, and use of systems documentation controlled?**

A Electronic documents furnished with Syntistix ES software are present on the install CD which cannot be changed by the user. The CD has a part number which identifies the version of the documents present on the CD.

21 CFR Part 11 Subpart C – Electronic Signatures

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. Such controls shall include:

11.300 b Ensuring Periodic Checks/Recalls/Revisions of Identification Codes and Passwords.

Q **Does the system force passwords to be periodically changed and also enable ID/password combinations to be rendered inactive without losing the record of their historical use?**

A Syngistix ES software depends on the capabilities of the Windows® operating system to handle password access. Windows® has capabilities to force passwords to be changed periodically. If a user is removed from the system, records of his/her activities within the Syngistix log files are not removed and continue to be available for review.

11.300 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.

Q **Does the system provide notification of attempted unauthorized access and take preventive measures (e.g. lock a terminal after a specified number of failed attempts, retain card)?**

A Syngistix ES software depends on the capabilities of the Windows® operating system to prevent unauthorized access. Windows® can be configured to prevent access after a specified number of failed attempts to log in.

PerkinElmer, Inc.
940 Winter Street
Waltham, MA 02451 USA
P: (800) 762-4000 or
(+1) 203-925-4602
www.perkinelmer.com

PerkinElmer®

For a complete listing of our global offices, visit www.perkinelmer.com/ContactUs

013736_01 PKI