Support for 21 CFR Part 11 and Annex 11 Compliance: Agilent ICP Expert software and SDA/SCM

White paper

Overview

Part 11 in Title 21 of the US Code of Federal Regulations (commonly referred to as 21 CFR Part 11) governs food and drugs in the US, and includes the US Federal guidelines for storing and protecting electronic records and applying electronic signatures. The equivalent guidelines in the European Union are defined in EU Annex 11.

The purpose of these regulations is to ensure the security, integrity and traceability of electronic records, which includes method information, data, analytical reports and other records (such as daily performance checks) asssociated with the operation of an analytical instrument.

Agilent's 5110 ICP-OES instruments are controlled by ICP Expert software. Agilent ICP Expert (version 7.X and later), when combined with two of Agilent's other software products: Spectroscopy Configuration Manager (SCM) and Spectroscopy Database Administrator (SDA) offers the functionality required to support compliance with 21 CFR Part 11 and Annex 11.

Agilent Technologies

This document examines each section of the 21 CFR Part 11 guidelines and provides a recommended approach using Agilent's ICP-OES products. It also addresses other commonly requested fucntionality for managing electronic records

The use of Agilent ICP Expert 7.X in conjunction with SCM/SDA provides a support framework for users to meet the compliance requirements mandated for a closed system. The system allows for the complete and accurate storage and recovery of records, and provides the capability for administrative control over user accounts, passwords and the privilege of users to perform various functions within the instrument software.

The system associates all users of the software with a unique user identification and password combination, which must be entered by a user and verified by the system before access to the instrument software is permitted. Security is further enhanced by the implementation of electronic signature functionality, requiring users to sign for changes to methods or other actions taken within the instrument software. All such changes, and the details of the user who made them, are recorded in a user-independent, unalterable, timestamped audit trail which is permanently associated with the worksheet to which the changes were made.

Security settings can be customised upon installation by system administrators to ensure that settings meet any specific requirements of organisational operating procedures and security guidelines. Customisable settings include user and group-specific access to functionality within the instrument software, user password length and history requirements, and analysis data storage locations. In this way, multiple projects can be managed and the users, permission sets and analytical data collected for each can be kept separate and secure within a single installation of the system.

Details of the system design and configuration options are outlined in the document, Agilent Spectroscopy Configuration Manager (SCM) Software: 21 CFR Part 11 Compliance Booklet (part number G9292-90031) available with the installation media. Further information on installation scenarios is available in the Software Installation Instructions for 21 CFR Part 11 Environments (part number G9292-90049). In addition to the instructions available with the software, Agilent provides a basic familiarization during the installation of the product for system users to aid in the transition to 21 CFR Part 11 compliance. Training courses for administrators as well as users are available.

Compliance for Agilent ICP-OES Systems

Compliance with regulations is a key aspect of an analytical laboratory's operation in pharmaceutical manufacturing.
The 4 components of compliance related to analytical instruments are:

- Design qualification (DQ), manufacturing quality control, lifecycle management and documentation, installation and operational qualification (IQ/OQ) for analytical instruments and their software.

- Control of user access to the workstation for instrument control and data processing (restricted user logon access with password protection)

- Electronic records security, integrity and traceability (secure storage, file versioning, audit trail, electronic signatures and archive/retrieval)

- Control of system operation, performance verification (PQ), physical access to laboratory and associated equipment, Standard Operating Procedures, training and records

Design Qualification
Regulated laboratories must ensure that equipment they use has been designed, manufactured, tested, installed and qualified under an acceptable Quality Process. In the case of instrument software, this means that the instrument manufacturer must be able to provide a declaration of Product Validation to confirm that their product supports user requirements for certification under 21 CFR 58 (Good Laboratory Practice), 21 CFR 210 (Good Manufacturing Practice for Drugs), or 21 CFR 211 (current Good Manufacturing Practice for finished pharmaceuticals). In Europe the equivalent GxP requirements are covered by ISO standards and ICH guidelines Q8, Q9 and Q10. An example of the declaration of Product Validation for Agilent's ICP-OES ICP Expert software is shown in Figure 1.

Figure 1. Examples of a Declaration of Production Validation (left) and IQ/OQ qualfication report cover sheets

Installation and Operation Qualification (IQ/OQ)

Once delivered to a user's laboratory, further qualification checks must be carried out to ensure that the delivered products match the specified items and that the system hardware and software functions as intended by the manufacturer.

These services are typically performed by the manufacturer and are referred to as the Installation Qualification (IQ) and Operational Qualification (OQ). IQ/OQ services should be available for the instrument system hardware and for all the software components required to operate it.

Examples of IQ/OQ documents for ICP-OES hardware and software can be seen in Figure 1.

Performance Documentation

The responsible personnel in the user organisation must setup appropriate controls on laboratory access, ensure that analytical performance is verified for the intended method and document the procedures to be followed for routine operations.

Once the equipment is installed and qualified analytical checks, known as System Suitability Testing (SST) are typically performed using the methods and samples that will be measured routinely. SST's confirm that the system performance meets the lab's specific analytical requirements.

Standard Operating Procedures are required to form a complete solution for pharmaceutical testing according to USP <232> and ICH Q3D and these will need to be created. Agilent manuals can contribute to the user collating an SOP. Other related products and services such as sample preparation equipment and certified calibration standards can also be supplied to provide and end to end workflow based approach to setting up the new analytical facility.

User access and electronic records

Software packages usually control and monitor access to the workstation and provide a secure integrated system for handling the data and other electronic records generated during the labs activities.

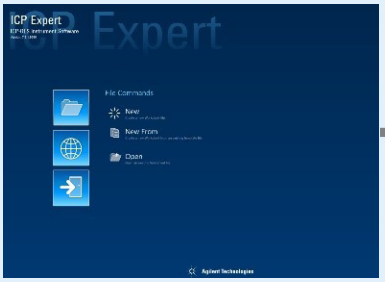
These functions are supported by the Spectroscopy Configuration Manager (SCM) for ICP Expert together with Spectroscopy Database Administrator (SDA).

ICP Expert with SCM and SDA

The software components that provide compliant operation for Agilent ICP-OES instruments are illustrated below in Figure 2. There are multiple installation scenarios for the software ranging from a simple installation where all software components are installed on the instrument control PC through to various distributed installations on networked servers*. Document number G9292-90049 provides more information on recommended installation scenarios.

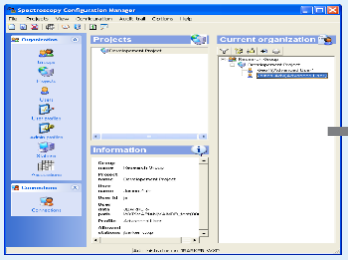
*Testing has been performed on specific servers. See document Agilent Spectroscopy Configuration Manager System Requirements, document number G9292-90047 for more information on servers supported for distributed installation scenarios.

ICP Expert software



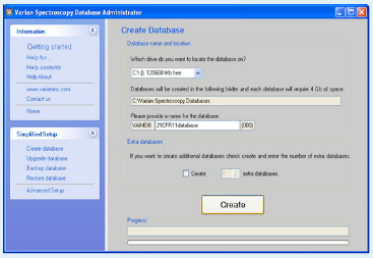
Application software controls the instrument for data acquisition and (re)processing

Spectroscopy Configuration Manager



SCM provides security with configurable, multi-level, password protected user profiles. Records user logon/ log-off and actions in audit trail

Spectroscopy Database Administrator



Databases are created by SDA and accessed by the application software. SDA uses Microsoft® SQL Server 2008 R2

Meeting the Regulatory Requirements of 21 CFR Part 11 with Agilent's ICP-OES software

The following table describes how the features and functionality of Agilent ICP Expert 7.X with SCM and SDA assists laboratories to meet the regulatory requirements of 21 CFR Part 11.

Section of Part 11 or other	Requirement	Yes/No	If yes, how, specifically, is the requirement satisfied, or, if no, what is the recommendation to users?
Validation			
11.10 (a)	Quality management system supporting the system validation. Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Yes	Agilent develops its products as per the well-established "product lifecycle" concept, which is a phase review process for software and hardware development, to ensure consistent product quality. This process requires the system to be subjected to an evaluation process before release to ensure software features and capabilities have consistent and intended performance. Agilent delivers a fully qualified data handling system together with all necessary services, which are needed to implement such a system to meet the requirements of the FDA regarding 21CFR Part 11. A validation certificate is provided with each copy of the software. Electronic records generated by ICP Expert are stored in a protected proprietary format using a secure algorithm. If such a record is altered through another application, this will be detected by the system when trying to read the record.
Accurate Copies and Secure Retention and Retrieval of Records			
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 FDA.	Yes	The system can generate accurate and complete copies of all records. Specifically, all method and data files generated by ICP Expert are stored in the SDA database as complete files in the original format. The method and data file includes the electronic record, data, method audit trail, operator identification and electronic signatures and can be loaded at any time using the ICP Expert software on a client PC, as a copy of the original data for review or inspection by the FDA. "Printed" reports are traceable to the original electronic files.
11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Yes	Records generated by ICP Expert are stored in the SDA database. Once stored, records are protected against modification or deletion. The SCM/SDA has been designed so that any results, data or methods information generated by ICP Expert are automatically stored in the SDA database. Data stored in the SDA database resides in a protected storage location or archive. Additional procedural controls should be defined and implemented by the system administrator based on company-wide security policies to manage practices such as archiving and server maintenance, access to client computers and password policy management. Records can be retrieved at any time by a user with the appropriate access privileges to the application.
Authorized Access to Systems, Functions, and Data			
11.10 (d)	System access is limited to authorized individuals.	Yes	Access to the system is dependent on a user entering a valid and unique combination of user identification and password. User credentials are created at the discretion of the system administrator, and can be altered or revoked by that administrator at any time. The system supports the enforcing of password requirements, such as length, reuse of previous passwords, and password aging. All login attempts, whether successful or not, are recorded in the system audit trail. Further to this, the system supports the assigning of varying levels of application privilege to different users or user groups, allowing a fine level of control over what specific users can do within the software.

Electronic Audit Trail			
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.	Yes	All actions relating to creating, deleting or modifying electronic records are logged in a secure, computer-generated, time-stamped audit trail. This audit trail lists all modifications which have occurred, as well as the identification of the user who made them, the time at which they were made, and a reason for the change if applicable. Entries in the audit trail are user-independent, and cannot be modified or deleted. Separate audit trails are available for the ICP Expert software and the SCM. New audit trail entries are recorded in addition to previous entries, with previous entries always remaining visible to users.
Operational and Device Checks			
11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Yes	When a sequencing of events is required, system checks enforce it. A few examples are: • If only approved methods are to be used in QA/QC, this can be achieved by restricting user access to the approved methods stored in the SDA database. • Within ICP Expert, sequencing of events are enforced with regards to electronic records in that the software ensures that required settings and facilities are available before allowing data to be collected and analysed, or ensuring files are saved before ICP Expert is closed. All events within the system are ordered and time stamped within the audit trail.
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.	Yes	Users cannot gain access to ICP Expert or to SCM/SDA without a valid user ID, password and account. Only a successful logon to the system offers access to files and general software functionality, instrument software functions or archival and approval functionality. The user must authenticate with a valid user ID, password and account. This applies at application initiation and after every inactivity timeout or manual logout. User access to specific functionality in the software is further restricted by the privileges assigned to the individual user. These privileges can be combined into roles if necessary. Upon entry of a user ID and password, the system checks the user ID, password, group and project and whether the given password is valid and in accordance with the defined account policies and password settings.
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.	Yes	Access to the instrument is limited to the configured device only. The system can recognize instrument models and serial numbers and uses proprietary binary communications. The instrument type, firmware revision number and serial number are passed from the ICP-OES to the ICP Expert software. The instrument serial number is recorded in the ICP Expert report, which is stored in the SDA database. Qualification of the software must be executed to ensure that devices and software are functioning properly.
11.10 (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.	Yes	Records of the educational and employment history of Agilent employees are verified and can be made available during an on-site audit. In addition, all relevant Agilent employees have attended training workshops for regulatory requirements.It is the responsibility of the organisation using the system to ensure that users working with the system have the education, training and experience required to perform their tasks. Agilent provides a basic familiarization during the installation of the product for system users. Training courses for administrators as well as users are available.
11.10 (j)	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, to deter record and signature falsification.	N/A	It is the responsibility of the organization implementing e-signatures to develop written policies which ensure that individuals responsible for signing documents understand that their electronic signature is as equally binding as their handwritten signature.
11.10 (k) (1)	Use of adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	N/A	While documentation is available for the users and administrators of the system, controls over the storage and distribution of this material are the responsibility of the organization that implements and uses the system.

11.10 (k) (2)	Use of revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Yes	Agilent's quality process includes written formal revision and change control procedures for system documentation. All revisions to the documents kept are time stamped and an audit is created.
Controls for open systems			
11.30	Procedures and controls must be used to protect the authenticity, integrity and confidentiality of the electronic records from their creation point to the point of their receipt.	N/A	The system is a closed system
11.30	Additional measures should be used to ensure the confidentiality of the electronic records from the point of their creation to	N/A	The system is a closed system
Electronic signatures - signature manifestations			
11.50 (a)	Signed electronic records contain information associated with the signing that clearly indicates: the printed name of the signer, the date and time when the signature was executed, and the meaning associated with the signature.	Yes	ICP Expert results can be electronically signed and approved by users assigned specific Approval privileges. The electronic signature and approval manifestation includes: • User ID in addition to the full name of the signer • Signer's title or profile • Date and time that the signature was applied • User-configurable meaning associated with the signature All signatures are saved with the result file, and are unalterable.
11.5 (b)	These items form part of any human readable form of the electronic record.	Yes	Electronic signatures will appear in ICP Expert result reports, which can be both displayed electronically and printed.
7. Signature/record linking			
11.7	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.	Yes	Within ICP Expert, signatures and approvals can be entered and require a system checked user ID and password. Electronic signatures cannot be transferred from one record or file to another, including the automatic entry in the application audit trail, which is always saved with the electronic record.
Electronic signatures - general requirements			
11.100 (a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Yes	The ICP Expert signature and approval tool employs two distinct identification components: unique user ID and password. Each user requires a unique and valid user identification and password.
11.100 (b)	Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	N/A	This is the responsibility of the organization that plans, implements and operates the system. Such a verification process is a system requirement that is set before implementing electronic signature procedures or assigning electronic signature privileges to an individual.
1.100 (c)	Has the organization delivered its declaration of e-signature use to FDA prior to or at the time of such use? Is it in paper form with a traditional handwritten signature? Can additional certification or testimony be provided so that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature?	N/A	It is the company's responsibility, before submitting electronically signed documentation to the FDA, to register their intent to use electronic signatures. In addition, training programs must be in place to ensure that users signing documents electronically understand the legal significance of their electronic signature.
Electronic signature components and controls			
11.200 (a) (i)	The e-signature must employ at least two distinct identification components, such as user ID and password.	Yes	The ICP Expert signature and approval tool employs two distinct identification components: unique user ID and password. Each user requires a unique and valid user identification and password. No two users can have the same user ID/password combination.

11.200 (a) (1) (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.	Yes	When an individual signs the first of a series of documents during a single period of controlled access, the user is required to enter both signature components: user ID and password. Each subsequent signing also requires the user to enter both signature components.
11.200 (a) (1) (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 the electronic signature components.	Yes	Each signature not performed during a continuous period of controlled system access requires all signature components.
11.200 (a) (2)	Controls should be in place to ensure that only their genuine owners can use an electronic signature.	Yes	ICP Expert used with the SCM/SDA can be configured so that an administrator assigns an initial password to a user for a new account or forgotten password, but the user is required to change that password on their first login. In this way, the user ID and password combination is known only to the individual. No two users can have the same user ID/password combination.
11.200 (a) (3)	Electronic signatures are 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.	Yes	ICP Expert used with the SCM/SDA can be configured so that an administrator assigns an initial password to a user for a new account or forgotten password, but the user is required to change that password on their first login. In this way, the user ID and password combination is known only to the individual. No two users can have the same user ID/password combination. The enforcement of this policy is the responsibility of the organization that operates the system. Therefore, it requires active collaboration with the purpose of sharing passwords to enable use of another users' identification.
11.200 (b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	N/A	The system does not currently support signatures based on biometrics.
Controls for identification codes/passwords			
11.300 (a)	Controls are in place to ensure the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password?	Yes	ICP Expert used with SCM/SDA requires users to authenticate with a user ID and password. Each user in the system must be unique and assigned to a specific user account. Each user requires a unique and valid user identification and password.
11.300 (b)	Controls are in place to ensure that the identification code and password issuance is periodically checked, recalled, and revised.	Yes	All aspects of password administration such as password aging, history and minimum length can be designated with the SCM. The administrator can define a timeframe in which passwords are periodically revised automatically. Users can be prevented from reusing passwords.
11.300 (c)	Loss management procedures are in place to electronically disable lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information.	N/A	The system does not currently support devices that bear or generate identification codes, such as tokens or cards.
11.300 (d)	Transaction safeguards are used to prevent un-authorized 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.	Yes	Only the user knows their user ID and password. Passwords are always displayed as asterisks and are stored encrypted so that even an administrator cannot see them. All attempts to access the system including both successful and unsuccessful logon attempts are recorded in the SCM System Audit Trail. The SCM user policy can be configured so that a defined number of failed access attempts locks out the user account.

11.300 (e)	Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information are in place to ensure that they function properly and have not been altered in an unauthorized manner.	N/A	The system does not currently support devices that bear or generate identification codes, such as tokens or cards.

Additional Functionality

In addition to meeting the regulatory requirements directly mandated by 21 CFR Part 11, Agilent ICP Expert software, in conjunction with the SCM/SDA software modules, has numerous additional features and capabilities which allow laboratories greater control over and confidence in the integrity of their analytical data.

Requirement	Compliant?	Specifics of compliance with Agilent ICP Expert 7.X used with SCM/SDA
The ability to install the administrative components of the system on a networked PC, physically separated from the location of the instrument control software.	Yes	The system allows for the SCM/SDA to be installed on a computer which is physically separated from the location of the ICP Expert software, connected over LAN. This installation method grants an additional level of data security, and allows for multiple instruments and installations of the ICP Expert software to be managed under one SCM/SDA installation.
The ability to permanently lock datasets after approvals have occurred, leaving the result data in a read-only state to prevent editing.	Yes	The system allows for ICP Expert worksheets to be permanently locked after results have been approved and signed off. This prevents any editing of the result data, and preserves the worksheet in the exact state it was in when the approval occurred.
The ability to backup and restore result databases to prevent data loss.	Yes	The system allows administrative users to perform a backup and restore of result databases where required. It is the responsibility of the organisation using the system to ensure that this is done in accordance with organisational operating procedures to prevent data loss.
Support for data migration from older or current versions of the system to future releases.	Yes	The system stores data in a format which allows results to be migrated from older versions of the system into newer versions, with no loss of data security or traceability. This will also apply to all future versions of the system which are released as compatible with ICP Expert 7. X.
System must prevent retesting or termination of testing prior to record creation without providing obvious indication to reviewer.	Yes	A sample cannot be re-run when using ICP Expert with SCM/SDA. This function is locked out with this combination of software. Premature termination of an analysis can occur but it cannot happen without existing data being saved.
The system must be configured to automatically log out or require login after period of inactivity.	Yes	The system can be configured to automatically log out the current user after a defined period of inactivity. No further actions can then be performed within the system until a user logs in and is authenticated.
The system is easily expandable to ensure enough storage capacity for collected data.	Yes	The SQL databases created for data storage within the system are sized at the discretion of the user. Multiple databases can be created and linked to the system. The allowable size of a database is restricted only by the storage space available on the relevant PC.

www.agilent.com/chem/pharma

Published May 22, 2017
Publication number: 5991-8143EN

Agilent Technologies