SDA COMPLIANCE SOFTWARE

For Agilent ICP-MS MassHunter Software

SDA Compliance Software Benefits

- Elemental Impurities in Pharmaceutical Manufacturing
- USP<232>/<233>
- SDA Software for ICP-MS delivers Compliance with 21CFR Part 11 for the Agilent 7700 ICP-MS and 8800 ICP-QQQ
- System Certification and Qualification Services (IQ/OQ)

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

Agilent's 7700 Series ICP-MS and 8800 ICP-QQQ instruments are controlled by ICP-MS MassHunter software. Earlier revisions of ICP-MS MassHunter supported integration with Agilent's OpenLAB ECM (Enterprise Content Manager) software to provide users with the tools to ensure compliance with these FDA regulations and their equivalent in other countries, such as Annex 11 in the European Union.

OpenLAB ECM remains an ideal compliance solution for large laboratories wishing to manage electronic records from multiple instruments and sites. But its cost and complexity may make it unsuitable for smaller laboratories that require a simple set of compliance tools to manage records from a single ICP-MS instrument.

The latest revision of ICP-MS MassHunter software (G7201B, B.01.02) for the 7700 Series ICP-MS and 8800 ICP-QQQ now also integrates with the Agilent Spectroscopy Database Administrator (SDA) software (G8499AA), to provide the tools to enable laboratories to comply with 21CFR Part 11. SDA is field-proven having been used for Agilent ICP-OES systems for several years. It is installed on the ICP-MS instrument workstation PC to provide a simple and cost-effective compliance solution for a single 7700 Series or 8800 ICP-QQQ instrument.

As with ECM integration, the control of user access to the ICP-MS MassHunter workstation, and recording of application and workstation audit trails is performed by ICP-MS MassHunter's User Access Control functionality (G7207B).

Compliance Overview

Compliance with Federal regulations is a key aspect of an analytical laboratory's operation in many industries, especially pharmaceutical manufacturers.

The 4 components of compliance related to analytical instruments are:

- Design qualification (DQ), manufacturing quality control, lifecycle management, installation and operational qualification (IQ/OQ) for analytical instruments and their software
- Control of access to the workstation for instrument control and data processing (restricted user access with password protection)
- Electronic records control (secure storage, file versioning, audit trail, electronic signatures, and archive/retrieval)
- Control of system operation, performance verification (PQ), physical access to the laboratory and associated equipment and records

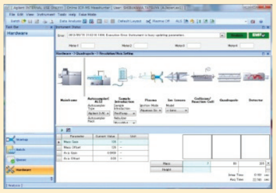
The first of these components must be demonstrated through the manufacturing quality records and equipment validation certification of the instrument manufacturer. The fourth component requires that the laboratory manager and administrators set up appropriate controls on laboratory access, and ensure that system suitability tests (SST) and standard operating procedures (SOP) are documented and followed.

The remaining 2 components (system access and control of electronic records) are typically controlled by software packages, comprising control and monitoring of user access to the workstation, and an integrated system for handling the data and other electronic records generated during the lab's activities.

ICP-MS MassHunter with SDA

The components of the ICP-MS/SDA software system that provides compliant operation for Agilent ICP-MS instruments are illustrated below. All software is installed on the standard ICP-MS MassHunter workstation PC, providing a simple and low-cost setup.

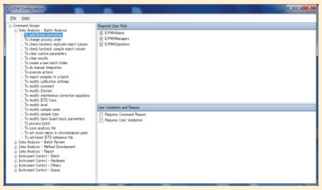
ICP-MS MassHunter
G7201B (rev.B.01.02)



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

+

User Access Control
(UAC) G7207B


ATM Configuration

File Help

Command Groups
- Data Analysis - Batch Analysis
  - To add/delete annotation
  - To change process order
  - To check/uncheck replicate reject column
  - To check/uncheck sample reject column
  - To clear custom parameters
  - To clear results
  - To create a new batch folder
  - To do manual integration
  - To execute actions
  - To import samples to a batch
  - To modify calibration settings
  - To modify comment
  - To modify Dilution
  - To modify interference correction equations
  - To modify ISTD Conc
  - To modify level
  - To modify sample name
  - To modify sample type
  - To modify Semi Quant basic parameters
  - To process batch
  - To save analysis file
  - To set noise region in chromatogram pane
  - To set/reset ISTD reference file
- Data Analysis - Batch Review
- Data Analysis - Method Development
- Data Analysis - Report
- Instrument Control - Batch
- Instrument Control - Hardware
- Instrument Control - Others
- Instrument Control - Queue

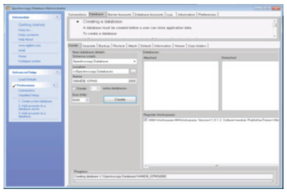
Required User Role
☑ ICPMHAdmin
☑ ICPMHManagers
☑ ICPMHOperators

User Validation and Reason
□ Requires Command Reason
□ Requires User Validation

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

+

SDA Software
G8499AA
ICP-MS MassHunter Version



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

Multi-level user access rights and audit trail settings (to define which users may perform certain functions and whether users must enter a password and reason to verify their access rights for those functions) can be configured by the laboratory Administrator, or the default Audit Trail Map (ATM) settings can be used. Database setup and administration is performed through the simple SDA configuration pane.

The following table describes how the features and functionality of ICP-MS MassHunter, in combination with UAC and SDA, enables laboratories to meet the regulatory requirements of 21 CFR Part 11.

Meeting the Regulatory Requirements of 21 CFR Part 11

11.10	Control for closed systems		
21 CFR Part 11	**Requirement**	**Result**	**Agilent ICP-MS SDA Software for 21 CFR Part11 Response**
11.10(a)	Has the system been validated in order to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records?	Yes	Agilent develops its products according to the well-established "product lifecycle" concept, which is a phase review process for software and hardware development, in order to ensure consistent product quality and conformity with regulation guidelines for product development. Agilent delivers a fully qualified data handling system together with all necessary services that are needed to implement such a system to meet the requirements of the FDA's 21CFR Part 11. The validation of the complete system is the responsibility of the user organization, which operates the system, and not of the software vendor.
11.10(b)	Is the system capable of generating accurate and complete copies of all required records in both human readable and electronic form suitable for inspection, review, and copying by the FDA or other regulatory agency?	Yes	MassHunter records (e.g. pdf files of tuning reports and concentration data reports) can be displayed using the applications provided with the software. Records and audit trails can be printed using predefined or user customized reports. SDA stores all data types, from raw machine data to resultant data reports. All files are stored complete and unaltered in the original format. "Printed" reports can be stored as PDF files which can be made available for review without the source application being installed on the client machine. Agilent SDA maintains the integrity of all data files.
11.10(c)	Are the records protected to enable their accurate and ready retrieval throughout the record retention period?	Yes	Data stored within SDA resides in a protected storage location. Regardless of the physical location of the data, it remains searchable to all users with appropriate privileges.
11.10(d)	Is system access limited to authorized individuals?	Yes	Data stored within SDA resides in a protected storage location. Regardless of the physical location of the data, it remains searchable to all users with appropriate privileges.
11.10(e)	Is there a secure, computer- generated audit trail that independently records 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.	Yes	Agilent MassHunter automatically generates time-stamped audit trails as a part of electronic record units to maintain a complete and accurate history of operation. Audit trails are used to record the actions of the operator in the Agilent MassHunter software and the SDA.
11.10(f)	Are operational system checks used to enforce permitted sequencing of steps and events, as appropriate?	Yes	In all functions, when a sequencing of events is required, system checks enforce it. For example, a method cannot be applied to data until the method has been validated for completeness. Users are prompted with an error message when steps are performed out of sequence.

11.10	Control for closed systems *continued*		
21 CFR Part 11	Requirement	Result	Agilent ICP-MS SDA Software for 21 CFR Part11 Response
11.10(g)	Are authority checks in place 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 the WorkStation PC or software system for acquisition or data processing without a valid user name, password and account. Once logged in, that user's access to files and software functionality (including but not limited to signing a file, inputting values, or altering a record) are determined by the privileges assigned.
11.10(h)	Are device (e.g., terminal) checks used to determine, as appropriate, the validity of the source of data input or operational instruction?	Yes	Instrument serial numbers are transferred from the ICP-MS instrument to the Agilent MassHunter software automatically. The serial number can be displayed on software, and it is recorded in the data file.
11.10(i)	Do the persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks?	N/A	This is the responsibility of the user organization that implements and uses the system, and should be controlled by procedures and documentation created by the organization.
11.10(j)	Have written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification, been established and followed?	N/A	This is the responsibility of the organization that implements and uses the system, and should be controlled by procedures and documentation created by the organization.
11.10(k)	Are there adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance?	N/A	While documentation for the operation and maintenance of the ICP-MS MassHunter/SDA system is available for users and administrators, control over the storage and distribution of this material is the responsibility of the organization that implements and uses the system.
11.10(l)	Are there formal revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of system documentation	Yes	Agilent Technologies' quality processes and product life cycle processes include formal written revision and change control procedures for system documentation. All controlled document revisions are time stamped and audit-trailed.

11.30	Control for open systems		
11.30	Are there procedures and controls used to protect the authenticity, integrity and confidentiality of the electronic records from their creation point to the point of their receipt?	N/A	Agilent MassHunter workstation is not designed to operate as an open system.

11.5	Signature manifestation		
11.50(a)	Do signed electronic records contain information associated with the signing that clearly indicates all of the following: • The printed name of the signer; • The date and time when the signature was executed; and • The meaning (such as review, approval, responsibility, or authorship) associated with the signature?	Yes	Electronic records contain the name of the user, the date and time, and the reason associated with the signing.
11.50(b)	Are these items subject to the same controls as for electronic records and included as part of any human readable form of the electronic record (such as electronic display or printout)?	Yes	Electronic signatures are subject to the same control as the record itself. Electronic signatures will be displayed on screen and in printout.

11.7	Signature/record linking		
21 CFR Part 11	Requirement	Result	Agilent ICP-MS SDA Software for 21 CFR Part11 Response
11.7	Are electronic signatures 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	Electronic signatures are unbreakably linked to the electronic record through software operations in the MassHunter Database Viewer.

11.100	Electronic signatures - general requirements		
11.100(a)	Is each electronic signature unique to one individual and not reused by, or reassigned to, anyone else?	N/A	This is the responsibility of the organization that implements and uses the system
11.100(b)	Are the identities of the individuals verified before the organization establishes, assigns, certifies, or otherwise sanctions an individual`s electronic signature, or any element of such electronic signature?	N/A	This is the responsibility of the organization that implements and uses the system
11.100(b)	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 hand-written 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	This is the responsibility of the organization that implements and uses the system

11.200	Electronic signature components and controls		
11.200(a) 1	Does the e-signature employ at least two distinct identification components such as user ID and password?	Yes	All users must be positively identified (authentication) before accessing the computer system (Operating System) or the application software. This is achieved via the combination of a unique user-ID, a personal, secret password and the user role based on the provided functionality/features of the PC operation system
11.200(a) 1(i)	When an individual executes a series of signings during a single, continuous period of controlled system access, is the first signing executed using all electronic signature components? Are subsequent signings 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 executes signings in any case, he/she always needs to execute the singing by using all of the electronic signature components, namely the combination of user ID and password.
11.200(a) 1 (ii)	When an individual executes one or more signings not performed during a single, continuous period of controlled system access, is signing executed using all of the electronic signature components?	Yes	When an individual executes signings in any case, he/she always needs to execute the singing by using all of the electronic signature components, namely the combination of user ID and password.
11.200(a) 2	Are controls in place to ensure that only their genuine owner can use the electronic signature?	N/A	This is the responsibility of the organization that implements and uses the system.
11.200(a) 3	Are the electronic signatures to be administered and executed to ensure that the attempted use of an individual’s electronic signature by anyone other than its genuine owner requires the collaboration of two or more individuals?	Yes	Both User-IDs and passwords are kept unique to users. Even the system administrator only knows User-IDs as he/she sets up the users. The password is only known to the individual users as it is defined at each user’s individual first logon. Thus this requires active collaboration with the purpose of sharing passwords to enable irregular use of somebody else’s identification.
11.200(b)	Are electronic signatures based on biometrics designed to ensure that only their genuine owners can use them?	N/A	Agilent has chosen to implement non-biometric.

11.3	Controls for identification codes/passwords		
21 CFR Part 11	**Requirement**	**Result**	**Agilent ICP-MS SDA Software for 21 CFR Part11 Response**
11.300(a)	Are controls 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-MS MassHunter uses Microsoft Windows User Group and Login ID, which ensures uniqueness of each combined identification code and password.
11.300(b)	Are controls in place to ensure that the identification code and password issuance is periodically checked, recalled and revised (e.g., to cover such events as password aging)?	Yes	ICP-MS MassHunter and SDA do not currently support devices that bear or generate identification codes, such as tokens or cards, as part of the security of the systems.
11.300(c)	Are there loss management procedures in place to electronically de-authorize 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?	N/A	ICP-MS MassHunter and SDA do not currently support devices that bear or generate identification codes, such as tokens or cards, as part of the security of the systems.
11.300(d)	Are transaction safeguards in place 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?	Yes	The administrator can safeguard the unauthorized login by setting the OS security policy, and the setting is applicable for the Agilent MassHunter software. The administrator is responsible for monitoring OS logs of all security violations, which include the following information: • the user-ID who created the violation • the date & time of the violation
11.300(e)	Are there controls in place to initially test devices that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized way?	N/A	Neither ICP-MS MassHunter nor SDA currently supports devices that bear or generate identification codes, such as tokens or cards.

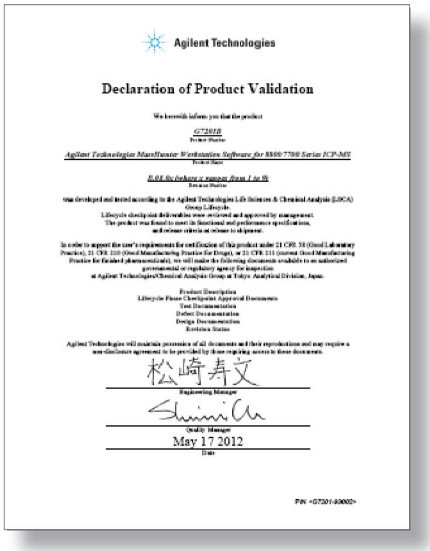
Descriptions taken from 21 CFR Part 11:
http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/cfrsearch.cfm?cfrpart=11

Certification and validation

Compliance Overview

Laboratories that are subject to Federal regulation must not only ensure that their routine activities are performed in a way that complies with the regulations, but also that the 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 software 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 finshed pharmaceuticals). An example of the Declaration of Product Validation for Agilent's ICP-MS MassHunter software is shown on the right.



Agilent Technologies

Declaration of Product Validation

We herewith inform you that the product

G7201B
Product Number

Agilent Technologies MassHunter Workstation Software for 8800/7700 Series ICP-MS
Product Name

B.01.0x (where x ranges from 1 to 9)
Revision Number

was developed and tested according to the Agilent Technologies Life Sciences & Chemical Analysis (LSCA) Group Lifecycle.
Lifecycle checkpoint deliverables were reviewed and approved by management.
The product was found to meet its functional and performance specifications,
and release criteria at release to shipment.

In order to support the user's requirements for certification of this product 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), we will make the following documents available to an authorized governmental or regulatory agency for inspection
at Agilent Technologies/Chemical Analysis Group at Tokyo Analytical Division, Japan.

Product Description
Lifecycle Phase Checkpoint Approval Documents
Test Documentation
Defect Documentation
Design Documentation
Revision Status

Agilent Technologies will maintain possession of all documents and their reproductions and may require a non-disclosure agreement to be provided by those requiring access to these documents.

松崎寿文
Engineering Manager

Quality Manager

May 17 2012
Date

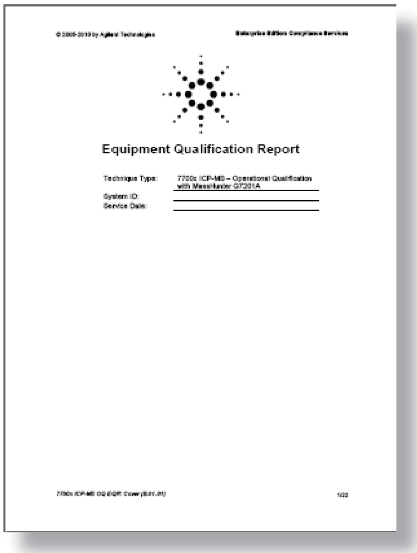
P/N <G7201-90002>

System Qualification (IQ/OQ)

Once delivered to a user's laboratory, further qualification checks must be made, to ensure that the products delivered match the specified items, and that the system hardware and software is tested to confirm it functions as defined by the manufacturer.

These services are typically performed by the manufacturer and are referred to as 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.

Further checks, known as System Suitability Testing (SST), are typically performed using the methods and samples that will be measured routinely, to confirm that system performance meets the analytical requirements. IQ/OQ documents for an Agilent ICP-MS and MassHunter are shown below.

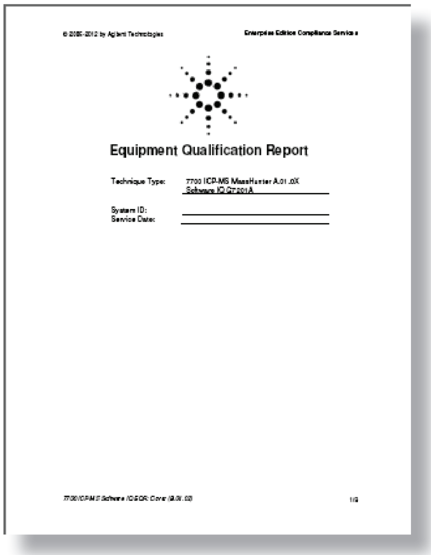


© 2005-2010 by Agilent Technologies
Enterprise Edition Compliance Services

Equipment Qualification Report

Technique Type: 7700x ICP-MS – Operational Qualification with MassHunter G7201A
System ID:
Service Date:

7700x ICP-MS OQ EQR: Cover (B.01.01)
1/22



© 2005-2012 by Agilent Technologies
Enterprise Edition Compliance Services

Equipment Qualification Report

Technique Type: 7700 ICP-MS MassHunter A.01.0X Software IQ G7201A
System ID:
Service Date:

7700 ICP-MS Software IQ EQR: Cover (B.01.02)
1/9

To learn more about Agilent SDA compliance
software for ICP-MS visit
www.agilent.com/chem/openlab

Agilent Technologies, Inc.
www.agilent.com

Published on April 1, 2013
5991-2002EN