Cerity Networked Data System for Pharmaceutical QA/QC

Revision A.02.01 and higher

Specifications

July 2003

Introduction

Cerity NDS for Pharmaceutical QA/QC is a fail-safe networked data system specifically designed for pharmaceutical QA/QC laboratories. It is powerful, flexible and utilizes an integrated client-server architecture enabling seamless industry standard distributed client-server scalability. Its user interface is optimized to model the way analysts work in the QA/QC environment, fully supporting their everyday tasks. Cerity NDS for Pharmaceutical QA/QC is available in two configurations.

Agilent Technologies

Table of Contents

Overview

Cerity NDS for Pharmaceutical QA/QC Professional

Cerity NDS Professional is the solution for laboratories that require instrument control, data acquisition, data analysis, flexible reporting and support for up to 8 chromatographs controlled by a single computer with strict adherence 21 CFR Part 11 (electronic records and electronic signatures) and related predicate rules such as to 21 CFR 210 (GMP) and 21 CFR Part 211 (cGMP). This configuration provides system access for one user at a time. It is designed for small laboratories that require secure data storage, data collection of electronic analytical records and support for several instruments without the need for concurrent user operations.

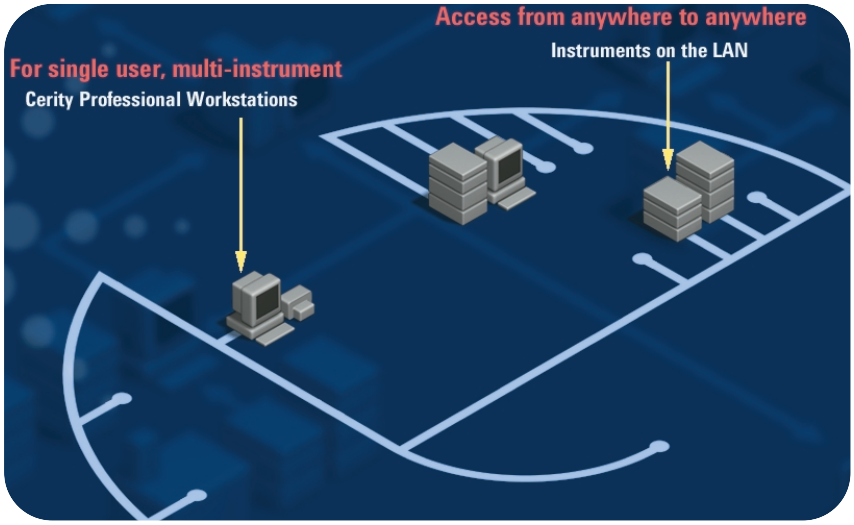


Figure 1
Cerity NDS for Pharmaceutical QA/QC Professional allows a single user to control, acquire and process data from up to 8 dual channel instruments.

The underlying technical infrastructure of Cerity Professional (e.g. processes, services and user interface components) is identical to the client/server configuration. A Cerity Professional system can be configured as a client in a Cerity client/server configuration.

Cerity NDS for Pharmaceutical QA/QC Client/Server

The Client/Server configuration extends the capabilities of Cerity Professional by distributing system tasks between the central database server, any number of connected instruments, acquisition controllers and review client workstations. This allows for multiple users to access and concurrently work with the central database and any connected instrument transparently from any connected client workstation. You can configure as many clients as necessary on the Cerity NDS system, considering any licensing and resource limitations.

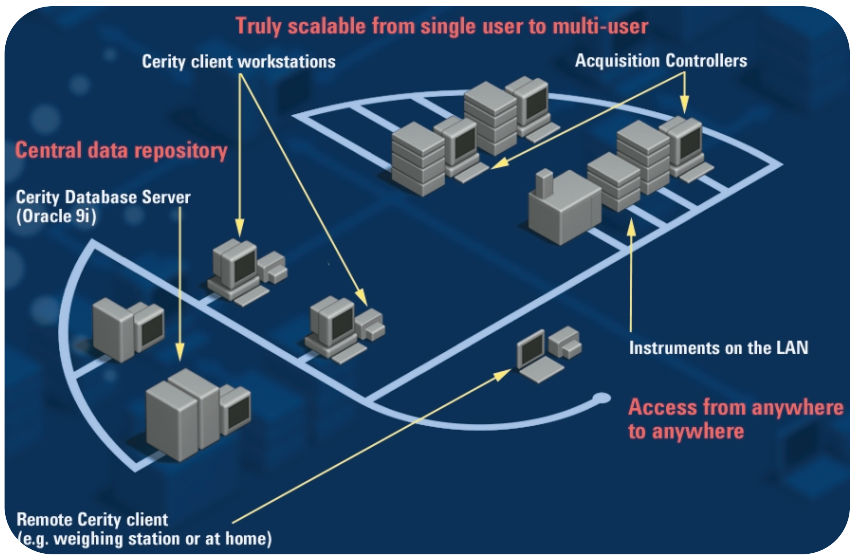


Figure 2
Example configuration of Cerity NDS for Pharmaceutical QA/QC Client/Server with one central Oracle database server and two groups of instruments controlled by dedicated acquisition controllers. Users access the system through the review client PCs.

General Description – Cerity NDS for Pharmaceutical QA/QC Client/Server

In a client/server environment, the Cerity NDS database server consists of a Microsoft Windows server hosting an Oracle database. This is the central data repository of the Cerity NDS system. The system includes the following networked components: database server, acquisition controllers, instruments, printers, client workstations and other devices. All raw data (acquired signals), meta-data (such as methods, calibration information, instrument serial numbers, calculation formulae), and calculated results are stored centrally in the database along with the computer-generated audit trail information.

Standard queries allow searching, retrieving and displaying data for review and other purposes, such as inspection, collation, sign-off and reporting.

The size of the database depends on the number of concurrent users, concurrent instruments and the amount of data online (accessible) in the database.

Data Acquisition and Instrument Control

Acquisition Controllers and Reprocessing Servers

Client/Server configurations allow the addition of optional acquisition controllers to balance instrument data stream and buffer it before upload to the central database server. The Cerity NDS acquisition controller is a dedicated Microsoft Windows Workstation running the Cerity NDS acquisition controller software. The acquisition controller performs data acquisition and instrument control. This component controls instruments that have been scheduled at the review client to execute an analysis using the specified method. It collects and processes the raw data and transmits it to the central database server. Acquisition controllers can theoretically be used as review clients. However, the background processing load on the acquisition controller typically decreases system performance for interactive use and is therefore not recommended for routine use.

Agilent Instrument Driver

The suite of drivers to control the supported instruments is bundled with the Cerity NDS software. The drivers for all supported instruments are installed with the base system. The supported instruments are the Agilent 1100 HPLC, the Agilent 6850 and 6890 GC, the Agilent 35900E A/D and the Waters Alliance 2690/2695 LC with a Waters 2487 Dual Wavelength Detector.

Agilent instruments implement Level 4 instrument control using standard LAN communications (TCP/IP). Cerity NDS controls instrument parameters and components and collects digital signals from detectors. Data can be acquired at rates up to 200Hz, the data rate required for fast GC and supported on the Agilent Gas Chromatographs.

Before the instruments can be used, they must be configured to an acquisition controller. One enabling Agilent instrument control license is required for each instrument. Instrument control licenses are available for the Agilent 1100 under Agilent product number G4061AA, the Agilent 6890/6850 GC under Agilent product number G4063AA and the Agilent 35900E Dual Channel Interface under Agilent product number G4064AA.

Waters Alliance Instrument Driver

Cerity NDS provides full instrument control of and data acquisition from the Waters Alliance 2690 and 2695 LC system. Instrument control of and data acquisition from the Waters Alliance LC require a direct connection between the computer and instrument, using an Agilent 82350 PCI high-performance GPIB interface adapter and cable. The standard interface control library software (SICL) required for GPIB communication is delivered with the Cerity NDS software. It must be installed on the acquisition controllers where the GPIB support is required.

A separate instrument control license (Agilent product number G4062AA) is required for each Waters Alliance HPLC system controlled by Cerity NDS for Pharmaceutical QA/QC.

Data Processing and Review

The Cerity NDS review client is the interface to the Cerity NDS system. Users perform their work with the graphical user interface (GUI) of the review client. Sample and sequence scheduling, instrument status monitoring, method setup, results review and approval and other tasks can be performed from the Cerity NDS review client.

Software Administration Console

The presentation of the GUI in the Cerity Software Administration module is made possible by integrating the Cerity Software Administration module with the Microsoft Management Console (MMC) and its user interface. MMC is a console designed to integrate management tools and functions and to present a common visual environment for management applications. Only operating system administrators can log on to the console. The Cerity Software Administration module permits administrators to set up system components, administer and track software licenses and license consumption, application modules, instruments, logon permissions, user capabilities and roles, auditing and system wide settings.

Network Infrastructure

Overview

The Cerity NDS infrastructure adheres to operating system and common IT standards. TCP/IP is the communication mechanism used by the Cerity NDS system. TCP/IP protocol accomplishes communication among network nodes, which includes analytical instruments, computers, network devices, etc. This is the primary protocol for communication among components in the Cerity NDS cluster. It is required on all Cerity NDS computers. Cerity NDS for Pharmaceutical QA/QC uses TCP/IP as delivered with the operating system.

Recommended Topology

Cerity acquisition controllers are designed to automatically reconnect to the required server resources (i.e. Cerity system services and the database). In order to protect instrument measurement analyses from LAN/WAN failures that affect the connection to the database server in the data center, Cerity acquisition controllers should be installed at the departmental level (i.e. on the same subnet as the instruments) and not in the data center.

Recommended Network Speed Settings

Available bandwidth settings and communication modes can vary, depending on the networking infrastructure, switches, and the network interface cards used in computers and instruments. Due to the lack of an established industry standard, auto-negotiation (auto-synchronization) of network speed settings has been reported to cause communication failures in some cases, especially where both computers and switches were configured to use this mode. It is recommended to use fixed speed settings, particularly for the network interface cards in computers and networked instruments. Generally, we recommend half-duplex mode for all network nodes as this setting will perform well both in switched and non-switched networks. Please note that full duplex mode may be used in switched network environments and if the hardware is compatible with this setting.

1. Servers are typically connected to the backbone through a main switch. The typical interface setting is 100MBit/s full duplex
2. Acquisition controllers should reside on the same subnet as the instruments. The recommended interface setting is 100MBit/s half duplex.
3. The recommended setting for PC clients for network speed is 100 MBit/s half duplex.
4. The network speed supported by analytical instrumentation-from Agilent depends on the exact model. The recommended setting for the Agilent 1100 HPLC, 6850 GC and the 35900E Dual Channel Interface, is 100MBit/s half duplex. The Agilent 6890N Gas Chromatograph, is only supported at 10 MBit/s half duplex.

A simple recommendation is to set the network speed for all analytical instruments to 10MBit/s half duplex. This allows moving instruments in the lab.

5. Network ports on the switches need to match the speed settings described above.
   If fixed speed settings are not in line with existing IT procedures and practices, switches may use "autonegotiate".

Network Interfaces

To connect Agilent Technologies instruments to an Agilent Technologies Cerity NDS for Pharmaceutical QA/QC system, an HP JetDirect Connectivity Card is required. The next table lists all HP JetDirect Connectivity Cards supported with the Cerity NDS for Pharmaceutical QA/QC software.

Agilent P/N LC	Agilent P/N GC	Description	Minimum FW
N/A	N/A	HP J2552B MIO card for 10Base-T, 10Base2	A.08.32
G1846A	G1847A	HP JetDirect 400N (MIO) card for 10Base-T, 10Base2, 100Base-TX	K.08.32

Table 1
HP JetDirect Connectivity Cards supported with Cerity NDS for Pharmaceutical QA/QC software

Assignment of IP Addresses

- The system requires a static IP address for the database server module, which is installed by selecting the Cerity Professional or Cerity Database Server installation.
- IP addresses for clients, acquisition controllers and instruments may be allocated statically by using the Bootstrap Protocol BOOTP, or dynamically using the Dynamic Host Configuration Protocol DHCP.
- The Cerity NDS system includes a dedicated BOOTP server which operates as a service in Windows. The Agilent BOOTP service should be used if no other BOOTP server or DHCP server are available to assign IP addresses to networked instrumentation and clients.
- The instrument configuration requires specific buffer settings on the Jetdirect interface card. These buffer settings are automatically configured by the Cerity Software
- If fixed IP addresses are available and assignment via BOOTP or DHCP from a server is not required, the Agilent 1100 HPLC and the Agilent 6890/6850 GC allow setting instrument IP addresses from the handheld controller or local keyboard.

Support for Failure Resilience

Support for Clustering (Server Failover)

Cerity for Pharmaceutical QA/QC supports clustering in the so-called "Active-Passive Mode", which is also referred to as "Active-Standby". All Cerity permanent data is held on the shared storage in addition to the so-called quorum information needed by Microsoft clustering.

Microsoft Windows 2000 Advanced Server provides clustering at the operating system level. Microsoft Cluster Server (MSCS) runs services required for cluster operation. In an active- passive cluster, two servers (nodes) share access to an external storage. Both computers can see the data in the shared storage, but only one of the nodes is active while the other is effectively on standby, waiting to take over if the primary (and active) computer fails to respond. Both servers have physical IP addresses as well as hostnames by which they can be reached through the computer network. In addition, a separate virtual IP address and machine name are configured for the cluster. The virtual address is used to access the active physical node of the cluster. Required system services run on the active node during normal operation. In the case of a failover, those services are started on the inactive node.

Oracle Fail Safe (OFS) services make the Oracle RDBMS cluster-aware and interact with the operating system to respond to failover system events. OFS ensures data integrity on the permanent data store in a failover scenario. OFS is an optional utility available for Oracle 9i.

Cerity A.02.01 SR1 and higher support both MSCS and OFS.

Oracle Enterprise Edition-specific functionality such as the Transparent Application Failover (TAF) and optional packages such as Real Application Clustering (RAC) provide additional support to handle in-flight data or database replication. These features are not supported by the Cerity NDS software.

Cerity Database Server
Cerity system services do not interact directly with the operating system to manage clustering related events. Instead, Cerity respond to cluster failover scenarios through MSCS. Cerity services running on acquisition controllers and clients automatically reconnect to the database server cluster after the failover is completed. Typical failover delays have been measured at less than one minute. Cerity acquisition buffering functions may be triggered during the failover delay.

A working failover cluster configuration requires that all Oracle data files as well as the Cerity report storage be located on the shared storage of the cluster server. Increased hardware resources should be specified as per Microsoft recommendations. Specifically, a separate mirrored disk (a so-called quorum disk) is highly recommended.

Acquisition Controller
Cerity A.02.01 SR1 and higher support enhanced acquisition buffering for instrument measurement data. In the event of database connectivity loss, acquired data is buffered on the acquisition controllers, and automatically spooled to the database once the database connectivity is re-established. To minimize buffering requirements, data analysis is suspended in acquisition buffering mode. Data analysis results can be generated by reprocessing the buffered raw data. The Cerity system continues and completes all sequences running at the time of the network failure.

Supported Analytical Instrumentation

Agilent 1100 Series Liquid Chromatograph
Full (Level 4) instrument control of the Agilent 1100 Liquid Chromatograph via LAN interface. In revision A.02.01 and higher, the following modules are supported:

- Agilent 1100 Isocratic, Binary and Quaternary pumps
- Agilent 1100 VWD, MWD and DAD (in 2D-chromatography mode)
- Agilent 1100 standard and Thermostated Autosampler
- Agilent 1100 Thermostated Column Compartment
- Agilent 1100 Vacuum Degasser

NOTE: 3D-spectral data acquisition and evaluation from the Agilent 1100 DAD and FLD are scheduled for revision A.02.02.

Agilent P/N	Agilent 1100 Module Description	Minimum Firmware	Comment
G1310A	Isocratic Pump	A.05.04	
G1311A	Quaternary Pump	A.05.04	
G1312A	Binary Pump	A.05.04	
G1313A	Autosampler	A.05.04	A.05.05 for units with SN >= DE32132734 Or mainboard replaced after June 2003
G1329A	Thermostated Autosampler	A.05.04	
G1330A	Autosampler Cooling module	N/A	
G1314A	Variable Wavelength Detector (VWD)	A.05.04	Requires mainboard rev. B
G1315A	Diode Array Detector (DAD)	A.05.04	No spectra acquisition, up to 5 simultaneous signals; Requires mainboard rev. B
G1315B	Diode Array Detector (DAD)	A.05.04	
G1316A	Thermostated Column Compartment (TCC)	A.05.04	
G1322A	Online Degasser	N/A	
G1323B	Control Module	B.01.02	
G1365A	Multiple Wavelength Detector (MWD)	A.05.04	
G1365B	Multiple Wavelength Detector (MWD)	A.05.04	

Table 2
Supported Agilent 1100 Series LC modules

One Agilent 1100 LC instrument control license is required per Agilent 1100 LC system connected to the Cerity software.

A LAN interface is required for the Agilent 1100 system. The GPIB interface is not supported in Cerity NDS for Pharmaceutical QA/QC for this instrument.

Agilent 35900E Dual Channel Interface

This interface can be used to acquire up to two independent channels of data from instrumentation that is not directly controlled by the software. The Dual Channel Interface supports data rates up to 100 Hz. The Agilent 35900E Dual Channel Interface supports BCD-coded vial number and can be used to track the vial position of each injection from third party auto samplers in the software. One Agilent 35900E A/D instrument control license is required per Agilent 35900E dual channel interface connected to the Cerity software.

A LAN interface is required for the dual channel interface. The GPIB interface is not supported in Cerity NDS for Pharmaceutical QA/QC for this device, refer to table 3 for firmware requirements.

Agilent 6850 and 6890 Gas Chromatograph

Cerity NDS for Pharmaceutical QA/QC supports the Agilent 6890A, and 6890N (table 4).

A LAN interface is required for the Agilent GC. The GPIB interface is not supported in Cerity NDS for Pharmaceutical QA/QC for this instrument (table 5).

Agilent 6850 Gas Chromatograph

Cerity NDS for Pharmaceutical QA/QC supports the following 6850 GC hardware, refer to table 6.

P/N	Description	Firmware	Comment
35900E	A/D converter	E.01.02	Data acquisition, remote start/stop, BCD

Table 3
Minimum firmware requirements

Agilent 6890A GC	
Inlet:	EPC—S/S, EPC—P/P, EPC—COC
Column Inlet:	Front, Back, Unspecified
Column Outlet:	Front, Back, Other, MSD, AED
Oven:	High Ramp Rate
Detector:	AIB, EPC—FID, EPC-FPD, EPC-NPD, EPC—TCD, EPC—ECD, EPC—uECD
Cryo:	CO2, N2
Valves:	GSV, LSV, Multiposition, Switching,
Aux:	EPC, Temperature
Data Channels:	In revision A.02.01, dual simultaneous (“dual tower”) injection is not supported

Table 4
Supported 6890 GC configurations

Agilent P/N	Description	Firmware	Comment
G1530A	6890A GC	A.03.05	
G1530N	6890N GC	N.04.08	LAN Board FW 04.5BD
G2612A (Controller)		A.01.07	Via 6980 only
G2613A (Injector)	7683 Autosampler	A.10.04	Full control, dual simultaneous
G2614A (Tray)		A.01.02	injection not supported
G1512A (Controller)		A.01.12	Via 6980 only
G1513A (Injector)	7673 Autosampler	A.09.14	Full control, dual simultaneous
18596C (Tray)		N/A	injection not supported
7694E	Headspace	1.02B	Via 6980 only in standalone mode

Table 5
Agilent GC minimum firmware requirements

Agilent 6850 GC	
Injector:	G2613A/G2880A
Inlet:	Split/Splitless, Purge/Pack
Column Inlet:	Inlet, Unspecified
Column Outlet:	Detector, MSD
Detector:	FID, TCD
Cryo:	CO_2, N_2
Valves:	GSV, LSV, Multiposition, Switching
Aux:	Temperature
Data Channels:	1
Handheld controller	G2629A

Table 6
Cerity NDS for Pharmaceutical QA/QC supports the above mentioned 6850 GC hardware

Waters Alliance

Full control of the solvent delivery system, column heater and autosampler of the Waters 2690 and 2695 Alliance Liquid Chromatograph via GPIB interface (optionally available with the software). Up to four Waters Alliance chromatographs can be controlled through a single GPIB interface. Full control of the Waters 2487 Dual Wavelength Detector via GPIB interface. One instrument control license is required per Waters Alliance system (consisting of one Waters 2690/2695 Alliance mainframe and one Waters 2487 detector) connected to the Cerity software.

Model Number	Description	Firmware	Comment
Waters 2690	Waters Alliance	1.21	The Waters 2690 has also been tested successfully using rev. 2.0 of the 2695 firmware
Waters 2695	Waters Alliance	2.0 or higher	
Waters 2487	Waters Dual Wavelength Detector	1.01	

Table 7
Waters instrument minimum firmware requirements

A remote start-stop cable is required to synchronize the Waters detector with the LC. See Table 7 for firmware requirements.

Hardware Requirements

The data system consists of a personal computer (PC) and Agilent software. All hardware and peripherals must appear in the appropriate Microsoft Windows Compatibility Lists for the operating system. Cerity NDS for Pharmaceutical QA/QC is designed to run on computers that conform to the specifications listed below.

Cerity NDS for Pharmaceutical QA/QC Professional

Table 1 lists the minimum computer configuration that is supported for a Cerity NDS for Pharmaceutical QA/QC professional system. This next table provides a guideline for computer hardware specifications, such as the amount of random access memory (RAM), disk space measured in gigabytes (GB), central processing unit (CPU) speed measured in megahertz (MHz), etc.

Cerity NDS for Pharmaceutical QA/QC Client/Server

Database Server Configurations Overview

The following table specifies the minimum and recommended hardware configurations for a database server.

	Low end	High end
Specification	4 single channel instruments	8 single channel instruments
CPU	Pentium III, 600 MHz	Pentium III, 600 MHz
Memory	512 MB, 1GB virtual memory	1 GB, 1GB virtual memory
Disk	20 GB	40 GB
Display	1024 x 768 pixels, 65536 Colors	1024 x 768 pixels, 65536 Colors

Table 8
Recommended hardware configuration Cerity NDS Professional

	Small (Entry Level)	Medium	Large
Specification	≤ 20 instrument channels ≤ 10 concurrent users	≤ 70 instrument channels ≤ 20 concurrent users	> 70 instrument channels > 20 concurrent users
Estimated number of chromatograms in database	100.000	330.000	700.000
CPU	Pentium III, 1 GHz	Pentium III, 1 GHz Dual processor recommended for >50 instruments	Pentium III, 2x 1 GHz (dual processor mandatory)
Memory	1 GB	1.5 GB	2GB minimum, 3 GB recommended
Disk Space (based on number of samples in database, see, above)	8 GB: Operating System, Oracle/Cerity application (RAID1) 8 GB: Oracle Tablespace 25 GB: Blobs Tablespace	8 GB: Operating System, Oracle/Cerity application (RAID1) 20 GB: Oracle Tablespace 72 GB: Blobs Tablespace	8 GB: Operating System, Oracle/Cerity application (Raid1) 30 GB: Oracle Tablespace 150 GB: Oracle Tablespace
	40 GB: Temporary space for backup utility files, Archive Redo Log files, Archives (RAID 5)	120 GB: Temporary space for backup utility files, Archive Redo Log files, Archives (RAID 5)	180 GB: Temporary space for backup utility files, Archive Redo Log files, Archives (RAID 5)
Display	1024 x 768 pixels, 65536 Colors	1024 x 768 pixels, 65536 Colors	1024 x 768 pixels, 65536 Colors

Table 9
Minimum hardware requirements and recommended hardware configurations for Cerity NDS database server

NOTE:

- *It is NOT recommended to use the Cerity database server as a print server for the Review Client computers.*
- *It is not recommended to use the Cerity Database server for network administration services such as domain control (Primary Domain Controller PDC or Backup Domain Controller BDC).*
- *Consider additional disks and disk array storage for better performance and reliability. One or more Rack-Storage/12 arrays configured with 18Gbyte or 36Gbyte drives allow for larger database sizes and better performance by multiple RAID arrays for the different database I/O subroutines.*

Terminal Server Configurations

Table 10 specifies the minimum hardware requirements for distributing the Cerity NDS user interface through a dedicated Terminal Server. One or more Windows 2000 servers with Terminal Services and Citrix Metaframe XP can be configured to run the Cerity review client software. However, the terminal servers are not expected to run other software besides Cerity and cannot be configured in server farm.

Acquisition Controller

- For configurations with more than 8 instrument channels, it is recommended to install acquisition controllers separately from the database server.
- For typical system configurations with 150 channels or less, it is recommended to use one acquisition controllers for every 15 instrument channels.

CPU	Pentium III
Memory	Minimum: 256 MB (8 instruments), 512 MB (15 instruments) plus at least 1GB of virtual memory Recommended: 512 MB (8 instruments), 1024 MB (15 instruments) plus at least 2GB of virtual memory
Disk	20 GB
Display	1024 x 768, 65536 Colors

Table 10
Hardware prerequisites for Cerity NDS acquisition controller

CPU	Pentium III,
Memory	Minimum 128 MB, 256 MB recommended
Disk	8 GB
Display	1024 x 768, 65536 Colors

Table 11
Hardware prerequisites for Cerity NDS review client

- There is no hard-coded limit on the number of instrument channels that can be collected by a single acquisition controller. The recommended maximum number of chromatography signal channels for an acquisition controller is 15.
- Acquisition controllers can also be used to balance the reprocessing load within a distributed Cerity NDS installation. In this case, the acquisition controller serves as a dedicated reprocessing server.

1. Plan your client/server systems to that you use no more than 15 channels for each acquisition controller. For example, a 35900E with 2 channels configured and a DAD with all 5 signals configured leaves 8 available channels.
2. For large systems with a heavy processing load, add an additional acquisition controller for every 10 review clients in your client/server system to perform off-line reprocessing. Do not add any instruments to these systems.

Table 10 specifies the minimum hardware requirements for an acquisition controller.
If server computers are available for acquisition controllers, RAID controllers are recommended. Fast PCs with sufficient RAM and virtual memory are also acceptable. For system redundancy, please consider standby computers to be used in case of computer hardware failures.

Review Client

Review clients are workstations used for interactive entry of sample and sequence data, method entry and management, scheduling of analyses, data review, reporting and result approval.

Table 12 specifies the minimum hardware requirements for review a client. Keep in mind, as previously stated, the acquisition controller and review client may operate together on a computer. It is recommended to deploy dedicated acquisition controllers for optimum performance and load balancing in the Cerity NDS system.

Operating System/Software Requirements

The following table defines the operating system requirements for each of the Cerity NDS for pharmaceutical QA/QC components. Table 13 defines the third party required software revisions to properly operate Cerity NDS for pharmaceutical QA/QC client/server and professional systems. Any of these components is installed automatically during Cerity setup, except for the Oracle Database Management System (DBMS) which needs to be installed separately.

	Windows 2000 SP3[2] Professional	Windows 2000 SP3[3] Advanced Server	Microsoft Windows XP SP1/1a Professional
Cerity NDS for Pharmaceutical QA/QC Database Server	No	Yes	No
Cerity NDS for Pharmaceutical	Yes	Yes	Yes
Cerity NDS for Pharmaceutical QA/QC Review Client	Yes	Yes	Yes
Cerity NDS for Pharmaceutical QA/QC Acquisition Controllers	Yes	Yes	No
Cerity NDS for Pharmaceutical QA/QC Professional	Yes	Yes	No

Table 12
Cerity for Pharmaceutical QA/QC Operating System Requirements (A.02.01 SR1 and higher)[1]

[1] Cerity NDS for Pharmaceutical QA/QC is fully tested and supported on the US-English, Japanese, French, German, Italian, Japanese and Spanish versions of Windows. On non-US English versions of the operating system, language-specific hotfixes of the operating system may be required. Any mandatory hotfixes are supplied on the Cerity NDS CD media. For correct interpretation of numeric floating point entries, specific options need to be configured in Windows' regionalsettings. Please consult the software status bulletin and release notes (readme.txt) for more information on regional settings, number and date formats required for correct handling of floating point number input.
[2] When using Windows 2000 SP3, hotfix Q326407 is mandatory (delivered with the core software).
[3] As of June 2003, compatibility pre-tests have been performed with Microsoft Windows 2000 SP4 pre-release versions

Manufacturer	Product	Revision	Comment
Oracle	Oracle 9i DBMS	9.2.0.3.0	Shipped on product CD-ROM; needs to be installed separately. Oracle Standard 9i is contained on Cerity product CD #2 through 6.
Microsoft	Data Access Components (MDAC)	2.7	Included with product
Microsoft	Internet Explorer	6 SP1	Needs to be installed separately. Included on Cerity CD#1.
Agilent	SICL library	L.02.01	Required for the control of Waters Alliance Contained on product CD #1 .
Microsoft	Visual Basic	6.0 SP4	Runtime library
Microsoft	Visual C++	6.0 SP4	Runtime library

Table 13
Other software requirements for Cerity for Pharmaceutical QA/QC

Oracle Licensing

Cerity NDS for Pharmaceutical QA/QC uses the Oracle RDBMS to manage and store its records.

- The Oracle RDBMS software may only be installed and used if the appropriate software licenses have been purchased. You must possess an Oracle license for each user account ("named user") established in your Agilent Networked Data System valid for use with the Agilent NDS software.
- The base products of Cerity NDS for Pharmaceutical QA/QC (Agilent G4000AA and G4001AA) include 5 application specific named user Oracle client licenses. These licenses are subject to a restricted use license and can only be used in conjunction with the NDS application.
- Agilent provides support for included Oracle software according to the application requirements of the respective Agilent networked data system. Further software maintenance for Oracle software must be purchased separately
- Alternatively, you may purchase full use Oracle licenses from Oracle Co. or their authorized distribution partners.
- Each individual with a logon to the Cerity software requires a separate Oracle client license.
- Additional Oracle licenses, can be purchased using Agilent product number G1411A. Please note that Oracle licenses delivered by Agilent Technologies are application specific and may only be used within the context of the Agilent networked data system.

Cerity NDS for Pharmaceutical QA/QC License

The number of Cerity NDS concurrent licenses in use must not exceed the number of licenses installed, otherwise the license agreement is violated. Additional licenses are easy to order and easy to install. The Cerity NDS licenses float and are consumed by concurrent users. For the client/server configuration, there must be an equal number of Cerity NDS licenses as there are Cerity NDS concurrent users.

- Cerity NDS for Pharmaceutical QA/QC Professional (Agilent G4000AA) is a single-user system and includes one concurrent Cerity user license. The following restrictions apply:

- Only one Cerity user can be logged on to the computer at any given time.
- G4002AA, add concurrent Cerity NDS user, is not applicable to the professional system. If the professional system is used by different operators at different times, each individual user requires a separate named user license of Oracle Standard valid for the Agilent NDS family of products.

GMP Module License

- One GMP license is needed for each concurrent user license (Agilent G4002AA)
- The GMP module enables strict auditing, audit comments and e-signature.
- The GMP module also enforces a strict results review/approval process. This will ensure that analysts review their own results before a peer reviewer and finally, a final approval is given.
- This is an enabling license; no additional software is installed. The GMP module enables the audit node in the Cerity System Administration Console.

Note: Only one GMP license is needed in the professional system.

Instrument Control License

One instrument control license is required per instrument controlled by the Cerity NDS software. The licenses are easy to install, and they are monitored by the application. Cerity instrument control licenses are available for the following products:

- Agilent G4061AA for instrument control and data acquisition of the Agilent 1100 HPLC
- Agilent G4062AA for instrument control and data acquisition of the Waters Alliance LC
- Agilent G4063AA for instrument control and data acquisition of the Agilent 6890/6850 GC
- Agilent G4064AA for instrument control and data acquisition of the Agilent 35900E Dual Channel Interface

Installation Qualification Tool (IQT)

The Installation Qualification Tool is a computer-based qualification utility used to perform Installation Qualification (IQ) of the Cerity NDS for Pharmaceutical QA/QC system. Computer-based installation qualification protocols verify the completeness and intactness of the Agilent software installed on the PC. The computer-based installation qualification utility available for Cerity NDS for Pharmaceutical QA/QC reads required details from the system directly and inserts them into the document automatically. The utility provides input forms for details that cannot be extracted automatically from the system (software and hardware). The entry forms support further techniques for automated data entry such as bar coding. Execution of the software IQ protocol requires a valid IQ license. Without a valid license number, the final acceptance protocol cannot be generated.

Operation Qualification Tool (OQT)

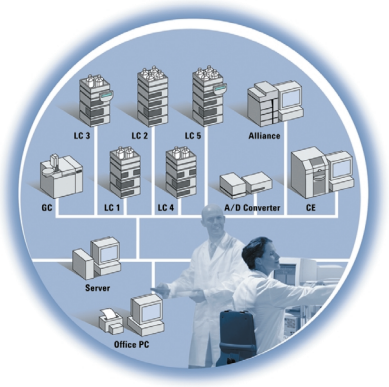
OQ allows qualification tests at defined intervals on the data system and the connected instruments. Without a valid OQ/PV test result, the system must not be used. OQ/PV typically requires a series of different tests depending on the instrument, the lab's specification and the configured software capabilities. System IQ and OQ/PV are provided both as a product and as a service from Agilent Technologies. The scope of the validation services and products for Cerity NDS includes the Agilent 1100 HPLC, Agilent 6890/6850 GC, Agilent 35900E A/D and software system qualification. The Operational Qualification Tool is a computer-based qualification utility used to perform Operational Qualification (OQ/PV) of the Cerity NDS for Pharmaceutical QA/QC system. The computer-based OQ protocols available for Cerity NDS for Pharmaceutical QA/QC uses well defined interfaces (so-called test harnesses) specifically designed into the software for the purpose of executing critical system test cases automatically. This comprises

- Automatic low and mid-level functional tests that verify fundamental system-level functions that are not even covered by the traditional interactive protocols available for other data systems
- Automatic high-level system operation tests that verify application functionality such as sequencing, quantification or recalibration. These tests execute in unattended mode and the evaluation is performed automatically using known data source, prerecorded acceptance limits and self-evaluating reports.
- A number of test cases require scripted manual tests because of their interactive nature. The test scripts cover areas such as challenging logon security, auditing of interactive changes, authority checks, and archive/restore functions.

Execution of the OQ protocols requires a valid OQ license. Without a valid license number, the final acceptance protocol cannot be generated.

Functional Specifications – Application

Technology and Architecture	
General description	Cerity NDS for Pharmaceutical QA/QC is a failure resilient, fully scaleable networked data system for analytical QA/QC laboratories that require chromatographic instrument control, data acquisition, data analysis, flexible reporting and with strict adherence 21 CFR Part 11 (electronic records and electronic signatures) and related predicate rules such as to 21 CFR 210 (GMP) and 21 CFR Part 211 (cGMP).
Description of data repository	Central, secure data repository based on Oracle database management system.
Supported Database Management System	**Oracle® 9i (9.2.0.3.0)**
Data Model	Object-relational data model.
Maximum size of data base supported	No hard-coded limits.
Design language/tools	UML, Visual C++, Visual Basic
Operating System	
A.02.01:	• Windows 2000 SP3 (Server, acquisition controllers) and Windows XP SP1/SP1a clients
A.02.01 SR 1 and higher:	• Professional, Server, acquisition controllers: Windows 2000 SP3 • Clients: Windows XP SP1/1a or Windows 2000 SP3 • Operation under Terminal Services (for clients only) • Microsoft clustering (DB server only)
Compatibility with Windows Terminal Server.	Client workstations of Cerity for Pharmaceutical QA/QC rev. A.01.03 and higher are supported for operation in a Windows 2000 Terminal Server environment. Thin client configurations are dictated by the Terminal Server provider (Citrix Metaframe or Microsoft) Agilent does not add any requirements unless specified otherwise. For details on the requirements and configurations of Cerity for Pharmaceutical QA/QC, please refer to a separate Technical Note, available as Agilent publication G4000-90100
Other client/server capabilities	• During running analyses, users can log out and log in without interruption of the sequence. • After log-out of the session, the user's license is released and available for another concurrent user.
Hardware requirements	See separate chapter in this document
Fail-safe	
	The Cerity system supports the following failure resilience mechanisms: • Server failover using Microsoft Cluster Server and Oracle Failsafe configurations to ensure continued uptime even if the server fails • Acquisition buffering on the acquisition controllers ensuring that no analysis data can be lost even if server/ network infrastructure fails.
Microsoft Windows 2000 Advanced Server Clustering	Supported in Active Standby mode
Oracle Failsafe (OFS)	Supported
Oracle Transparent Application Failover (TAF)	Not supported
Oracle Real Application Clustering (RAC)	Not supported



Scalability	
Cerity NDS for Pharmaceutical QA/QC Professional:	One user at any one time.
Maximum number of concurrent users	Note: By definition, Cerity NDS for Pharmaceutical QA/QC Professional is a single-user, multi-instrument configuration.
Cerity NDS for Pharmaceutical QA/QC Client/server :	No hard-coded limits (function of database server configuration and available network bandwidth);
Maximum number of concurrent users	Typical configurations have 30-50 users and 80-100 instruments.
User Interface	
Characteristics of the User Interface	Graphical user interface designed in adherence to Windows standards and configurable to laboratory specific workflow (based on user roles and analysis specific requirements). The user interface of Cerity NDS for Pharmaceutical QA/QC is streamlined to adhere to the requirements of GMP regulated QA/QC labs. This includes, but is not limited to • Convenient arrangement of functions into four context areas: Sample Entry, Instrument Status, Results Review and Method Management • Graphical Instrument Status Display • "Explorer"-like Tree-View to conveniently display search results from the database • Menus (pull-Down as well as context menus) • Toolbars • Tables configurable to the method
User specific storage of user interface configuration details (profiles)	Specific to job roles and analytical methods. If a user has no permission to use a certain system function, the function is not shown in the user interface or it is disabled (grayed out).
Analytical instruments	
Supported analytical techniques	LC, GC, A/D converter (general purpose)
Number of instruments that system can simultaneously control and acquire data from.	No hard-coded limits (function of database server configuration and available network bandwidth); Typical configurations have 30-50 users and 80-100 instruments.
Data acquisition interfaces	
LAN	Level 4 instrument control of 1100 LC, 6890/6850 GC and 35900E ADC, using TCP/IP protocol as installed with Microsoft Windows.
IEEE-488 (HP-IB/GP-IB)	Based on standard interface control library (SICL)
Level of bi-directional instrument control	Level 4 instrument control for instruments with appropriate capabilities (e.g. Agilent 1100 LC and Agilent 6890/6850 GC) Level 3 instrument control for Waters Alliance LC and the Waters 2487 Dual Wavelength Detector.
Instruments for which bi-directional control is supported.	Agilent 1100 Series LC, Agilent 6890/6850GC, Waters Alliance, Agilent 35900E ADC for general purpose/multi-vendor interfacing
Proprietary control hardware required?	No. Instruments interfaced via LAN require a HP JetDirect LAN interface and an Ethernet LAN card in the PC. Waters Alliance instruments are interfaced via GPIB (IEEE-488) and require an Agilent 82350 GPIB board in the PC

Network monitoring capabilities (computers and instruments)	The networked design of all components ensures that all parts of the system can be monitored as nodes on the network. Commercially available network monitoring tools allow to measure network bandwidth, network health, track errors and alerts and help in troubleshooting problems related to communication between computers and instruments on the network. Network monitoring tools cannot be used to monitor non-networked instruments using legacy connections such as GPIB or RS232.
Data Transfer	
Data import formats	• Data files from Agilent ChemStation A.03.01 or greater • ANDI (Analytical Data Interchange) format • Import of work-lists in XML format, e.g. from a LIMS.
Data export formats	• Microsoft Excel format (XLS) for tabular data • HTML for analytical reports • JPEG, GIF, TIFF, WMF for graphics • ANDI (Analytical Data Interchange) format • XML for export of archive catalog files (for use with knowledge management or archive management system)
Standard interface protocols supported between network components of the system	COM+/DCOM
Results review (o-line on-demand viewing)	By design, all result records are available for instantaneous online review in the results review context of the application.
Direct FAX or PDF output	Through standard operating system functions (print to fax, print to PDF device)
Other interfaces	Examples for further customization based on the following techniques • Reports post-processing through DOM (Document Object Model) • Reports post-processing through embedded scripts (Javascript or VBScript code) • Web-Access to queries through SSL (Secure Sockets Layer) • Programming interface (requires PSO consulting)
Documentation	
Description of documentation delivered with the Cerity system	• How-To Tasks (Online Help), • Cerity Quick Reference Card • Cerity Concepts Guide • Getting Started Cards • Cerity Installation Guide • System Administration Guide (Online, PDF) • Cerity Technical Reference Guide
Description of formats used for online documentation.	PDF and HTML Help
Number of printed manual sets provided with system	One set per user license *(Note: Additionally, PDF-versions of all manuals are included on the software media)*
Link to standard operating procedures SOPs	The application user interface allows to configure a link directly to the intranet location where SOPs or monograph are stored

Access Security and Control	
Security concept	Based on NT security system (user accounts management, password policy). Application does not have a proprietary account system but allows reusing password and security policies directly from the operating system.
Access controls for security configuration	User with Cerity system administrator permissions. *Note: Cerity system administrators require system administration permissions on the local computer*
Granularity of security access	Managed at the individual function level of the application. Menus and toolbar functions can be selectively configured for each user role. Examples: Create method, reprocess chromatogram, approve result etc.
Description of application security controls	• Cerity users must be authenticated through the operating system • Mandatory login using user-ID and password • Cerity uses a role-based security concept based on job roles and job responsibilities of users. • Prior to executing a function in the system, Cerity's security service checks whether the user has the appropriate capabilities • Mandatory audit trail every time a record is created, modified or destroyed • Cerity allows to configure which system tasks require authorization by electronic signature (e.g. accept/reject an analysis result). • System-wide inactivity time-out locks the session after a predefined idle period • Physical access security controls are not enforced by the application, but the system is compatible with physical access security controls such as bio-metric or smart-card identification as supported by the operating system.
Security mechanism of network data packets	Yes, using COM+ security
Biometrics-based identification	Planned for subsequent release: Support biometrics-based identification with standard interfaces for face recognition, voice recognition, fingerprint scanning
Instrument Status and Analysis Scheduling	
Instrument Status Monitoring	• Transparent real time access to any instrument connected to the net work, independent of the instrument and the client computer. • Transparent access to instrument control and equilibration functions such as reset injector, lamp on/off, balance detector, wavelength calibration

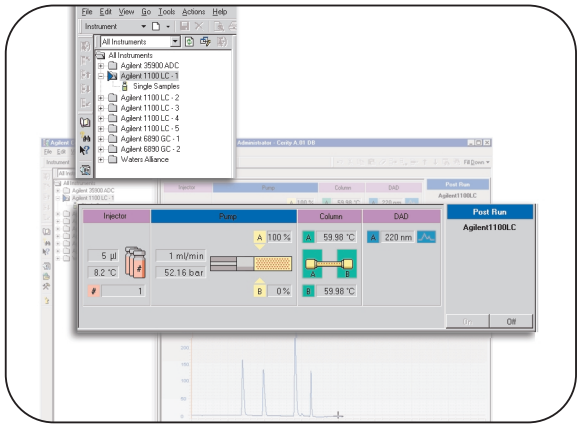
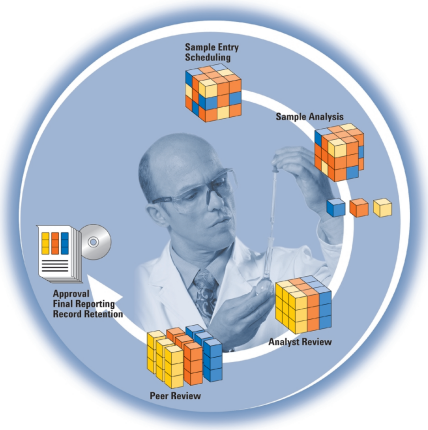


Figure 3
Transparent access to connected instruments

Real-time display	Configurable online plot for detector channels and diagnostic plots (e.g. thermostat temperature, pressure, flow)
Instrument actuals	Configurable status information table (run-time, instrument errors, warnings, diagnosis buffers)
Real-time status – finding out why the instrument is in an error state or not ready.	Cerity offers three troubleshooting mechanisms for problems such as: • instrument status GUI and instrument actuals • instrument logbook • "Service Report" function that queries the diagnostic registers of the Agilent 1100 Series to generate a service report that helps to diagnose instrument problems down to the module level
Scheduling of analyses ("chaining of analyses")	The system uses a scheduling process that allows submitting analysis jobs (single sample analyses as well as sequences) to the so-called worklist. The analysis priority is entered at sample entry and can be high, medium or low.
Sample/Sequence Entry	
Automatic data entry	A "Sequence Template" can be configured as part of the Cerity method. When creating a new sequence, the new sequence is pre-filled based on the settings defined in the sequence template stored in the analysis method.
Mechanisms to minimize typing effort during data entry	• Fill-down column • Intelligent fill-down wizard • Apply changes to a selection of sequence lines
Multiple stop times in sequence methods	New in A.02.01: The sequence template allows setting different analyis times ("stop times") for the different runs of a sequence. This is useful for cases where the analysis time for samples is significantly longer than for calibration standards.
Revision control of sample data	Sample data is subject to strict revision control within the application.
Entry of calibration standards	Weights (concentrations) of calibration standards can be directly entered during sample entry. Partial calibration and multi-vial standards are supported (standard compounds of a certain level can be provided in different vials)
Method specific sample variables	Method specific sample variables (multipliers, divisors) are entered during sample entry and available for custom calculations.
Custom naming of method specific sample variables	Yes, names are configurable per method.
Naming conventions allow for long descriptors	Names and description fields for samples, sequences, methods and instruments permit long descriptive names with at least 128 characters.
Operator can selectively run data acquisition, processing, reporting	When scheduling an analysis, operators can selectively define which processing tasks will be performed. Options include data acqusition, data analysis and reporting.
Method Management	
Change control to methods maintained in the data system	Cerity subjects all methods to strict revision control and audit trail logging. No part of the method can be overwritten.
Who needs to modify methods	Method management is typically only required for a senior chemist or chemist. Analysts (chemists, technicians) typically work with predefined methods.
Master methods (template methods)	Master methods are protected methods that serve as template for instrument specific methods. By using a master method, analysts can be sure that the analysis settings are coherent with the official analysis procedure.
Linking methods to analysis procedures	Cerity allows translating a chromatographic analysis procedure into a Cerity method. This includes the required sample entry variables, calculations, recalibration schemes, layout and reporting requirements and templates for the sequence of injections.

System checks to ensure consistency between method parameters and physical instrument capabilities	The software queries the current configuration details from the physical instrument prior to starting the analysis to ensure that the analysis parameters are compatible. Cerity methods are specific to an instrument configuration (e.g. Agilent 1100 Series LC with a DAD and a binary pump) and can be applied for groups of instruments that have the same configuration.
Typical interaction of an analyst with a method	• Login to system • Select sample entry context (view) • Login the sample • Select the method (the system automatically suggests the instrument suitable for this analysis) • Enter sample information (description, name, vial number, product code, LIMS ID, concentration of standard etc.) • Schedule analysis
Settings controlled by the Cerity method	• Sample variables (multipliers and divisors) • Limits • Example chromatogram (i.e. a typical chromatogram as generated with this analysis) for display in online results review and on reports • Instrument control/data acquisition • Integration • Peak identification • Calibration • Quantification • Custom calculations • Reporting • Data review layout • Reporting
Reintegration	• System allows reintegrating results in the controlled environment of Cerity results review context. • Fine-tuning of integration settings on a specific chromatogram is per formed under strict revision control of the result record. • Fine-tuning of integration settings on a specific chromatogram remain private to the chromatogram and do not implicitly affect the master method.
Reprocessing	• Reprocessing functions allow to reprocess data with modified parameters, or a different revision of the same method or a different method. • Reprocessing calculations are subject to audit trail and revision control functions of the software.
Data review layout	• The method stores so-called “data review layout” settings. • Data review layout defines the content and layout of the graphical and tabular display of results generated with a particular analysis method • The data review layout is used to show analysis results consistently in the application's result review context. • The result display is method specific and independent of the user and the client PC used for the review.
Sequence template	• The method allows storing the “Sequence Template”. • The sequence template defines the normal sequence of injections required for analyses run with this method: blank injections, system suitability, standards, samples, QC samples etc. • The sequence template of the method minimizes data entry effort during sequence setup.



Data Analysis	
Integration algorithm	Revised version of the Agilent Enhanced Integrator.
Integration events	The system allows setting integration events to change integration parameters appropriate for the signal measured during the analysis. Typical integration events include, but are not limited to: • Area reject • Height reject • Slope sensitivity • Peak width • Shoulder detection • Tangent skimming • Detection of negative peaks
Standard quantification modes	Area%, Norm%, External Standard Quantification (ESTD), Internal Standard Quantification (ISTD)
Description of recalibration schemes for sequence analyses	The system supports flexible calibration schemes: • Moving average calibration (single update calibration) • Standard bracketing • Overall bracketing (also known as “grand average bracketing”)
Description of overall bracketing calibration scheme	Two bracketing modes are available. Overall bracketing calculates one calibration curve per calibrated compound for the sequence and uses it for the quantification of all samples in the sequence. In terms of validation and traceability, this is a lot easier to handle than other floating average recalibration schemes.
Description how the system prevents discrepancies between printed reports and results displayed on the screen.	The Cerity report writer is a rendering device that only displays data already stored in the central data repository and does not perform any calculations of its own. This is to avoid discrepancies between results shown on screen and paper.
Description of how system controls re-integration and reprocessing in a controlled manner according to GMP and 21 CFR Part 11.	Every modification of a test result (e.g. in the course of reintegration or reprocessing using updated calibration information) results in a new revision of the result record along with tight links to the metadata and result. Manual intervention in the integration of a chromatogram is notified in the report and in the system's online results view using the following measures: • Definition of user capabilities for authorized access • Strict auditing with mandatory audit comments • Authorization by electronic signature (configurable) • Data review layout and Report templates set up to include analysis audit trail and method version
Support of method specific calculations	Yes, through spreadsheet integrated into the data analysis method.
Supported calculation functions	Arithmetic, logical, statistical functions also available in off-the-shelf spreadsheet programs.
Storage of method specific calculation results	Yes, including calculation formulae.
Triggering of warnings (pass/fail information) based on calculation results	Yes, such as warnings if system suitability or other limits are exceeded.
Description of user-defined (custom) calculations	The built-in Custom Calculator spreadsheet. This allows setting up method specific calculations, for individual peaks in a single injection, groups of compounds in groups of injections and even summary statistics for entire sequences.

Specialized calculation functions	Custom calculations for single injections, groups of injections and sequences are available in the custom calculator built into the data analysis method. Examples: • Impurity calculations • Reproducibility calculations for replicates • Group statistics • Response factor statistics (calibration precision)

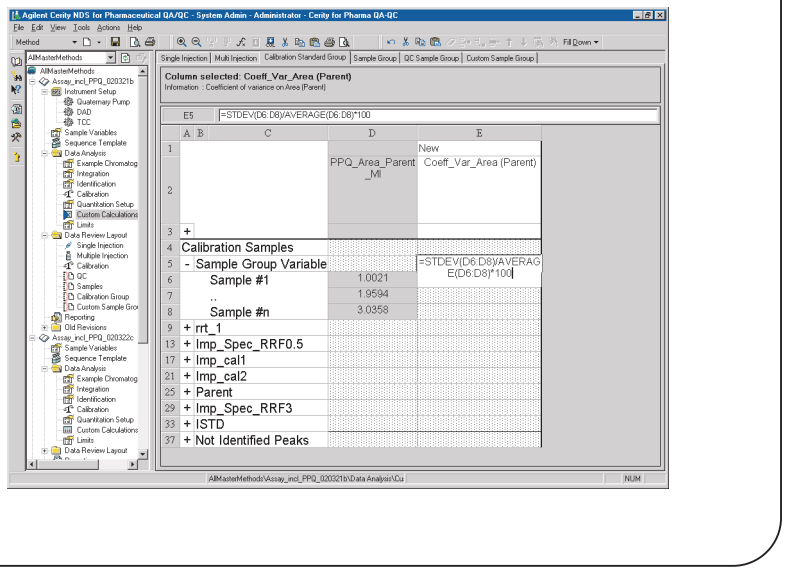


Figure 4
Setting up a method-specific statistical group calculation in the "Custom Calculator"

Description of system suitability criteria and limits.	• Cerity calculates peak performance parameters according to the different pharmacopoeias (USP, EP, BP, JP and DAB). The user can con figure which of them are reported and shown. • System suitability limits can be defined by component and sample type. • Available noise calculations: peak to peak and ASTM.
Description of peak identification mechanisms.	• The system supports identification by absolute and relative retention times (RRT). • Peak windows for peak recognition are customizable per peak using absolute or relative peak retention time windows. • Peak summing and peak grouping. • The system compensates for retention time variability during analyses using reference peaks for the RT update. • Peak naming is flexible and allows for long names. • Peak confirmation based on spectral data is planned for subsequent release.
Calibration capabilities	The system allows multilevel calibration with an unlimited number of levels, fixed amount, variable amount and manual response factors.
Reprocessing capabilities	All chromatographic runs in a sequence can be reprocessed automatically ("batch-wise").

Available calibration schemes	Cerity supports the following calibration curves types: piecewise, linear, quadratic, cubic, exponential, logarithmic, power, average slope. The following weightings are supported: • Equal • # of calibrations • Linear (x) – by the factor 1/Amount • Quadratic (x) – by the factor 1/Amount^2 • Linear (y) – by the factor 1/Response • Quadratic (y) – by the factor 1/Response^2 • Lg (x) – by the factor 1/lg(Amount) • Lg (y) – by the factor 1/lg(Response) • Ln(x) – by the factor 1/ln(Amount) • Ln (y) – by the factor 1/ln(Response)
Calibration curve origin treatment	• Include • Force • Ignore • Piecewise (connect)
Calibration review capabilities	• An authorized user can reject individual calibration points manually from a calibration curve; This action is subject to audit trail and requires authorization by electronic signature if configured so. • Calibration data display includes regression curve, correlation coefficients, confidence intervals (configurable) and relative residuals.
Quantification capabilities	• Response factors are calculated from the calibration result and stored automatically. • Response factors can also be entered manually per peak. • Response factors can be updated automatically after performing a re-calibration • Results can be calculated using a factor per peak in its calculations. • Results can be calculated using the same factor for all unknown impurities in its calculations. • Specified impurities can be calculated using a specific factor.
The systems allows to define and check limits on system suitability parameters.	• Cerity allows setting limits on all calculated values (including custom calculations). • Limits can be based on sample type. • Allows defining peak specific limits. • If a parameter is out of limit a user-defined action is performed (e.g. trigger configurable warning).

Online Results Review and Approval

Display of analysis results	• Online results review is a separate context (view) of the application.. • Results can be queried from the Cerity database using standard or customize queries (database searches). • Results are displayed according to the settings defined in the data review layout of the method.
Results approval	• The system supports a 3-step results approval process (analyst review, peer review, manager approval). • Data can be approved, rejected, or marked for rework. • Operational system checks ensure the approval steps are performed in permitted sequence of steps.

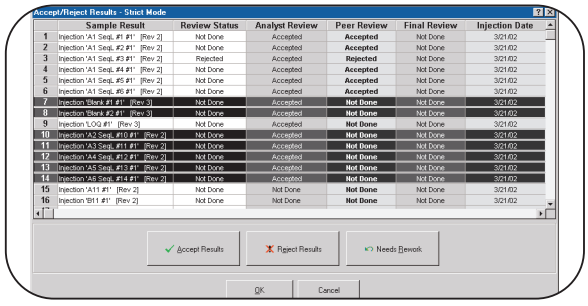


Figure 5
Result approval in the Accept/Reject screen for results sign-off

Description of retrieval capabilities	• Database queries can be defined with a query wizard to search for data. • Queries can be defined based on Samples, Methods, Instruments and results. • All results can be stored and retrieved.
Protection of electronic records managed by the system	All binary raw data is handled by the Oracle database and Cerity information manager objects and is under strict revision control of the Cerity security service.
The actual position of analyzed vials in auto-samplers is stored and reported (Part 11)	Yes, for Agilent 1100 Series LC and Waters Alliance LC. For 3rd party autosamplers, requires BCD vial number input to the 35900E.
All components of the system are identified in the system (Part 11)	Automatic tracking and storage of instrument serial numbers and firmware revisions (depends on instrument capabilities).

Reporting

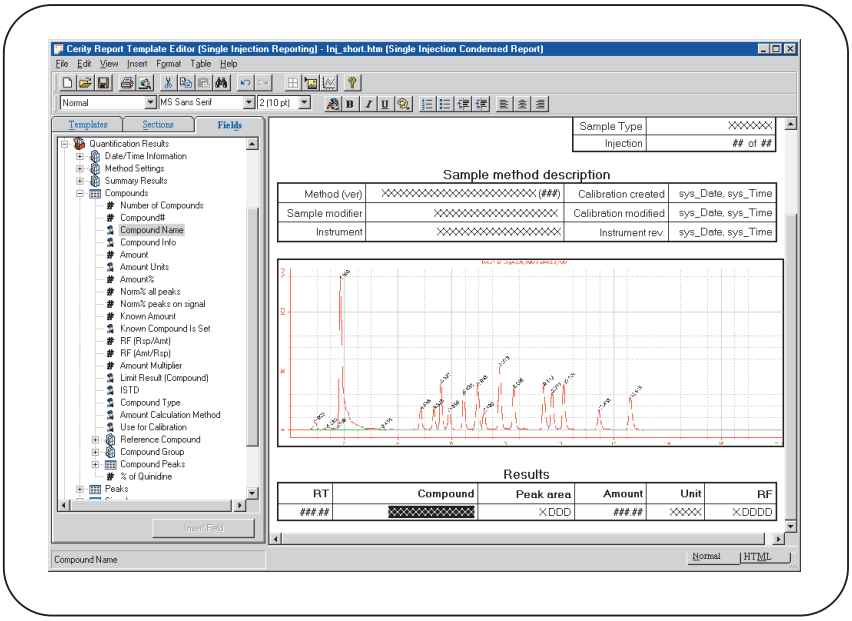


Figure 6
Example Report Template

Description of Cerity report generator	The reporting functions consist of a graphical report template editor and a reporting tool that extracts the data to be reported from the Cerity database. Report design is done through drag & drop editing of the report. Report templates are stored in HTML format. Reports can be published to a web browser and on paper.
Configurability of the report generator	• All Cerity reports can be customized using the report template editor. • Report template editor allows to render (visualize) all data from the application database. • Item selection is done using a tree view representation of the system's "data dictionary"

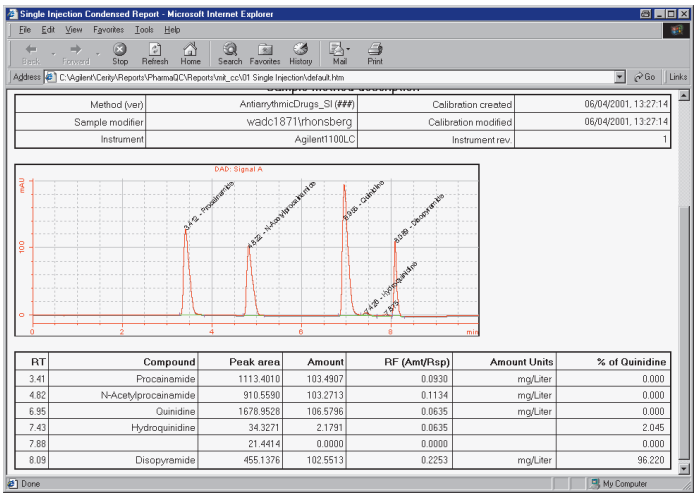


Figure 7
Example Report Published in a Web Browser

Description of built in reports	Single injection reports, group summary, composite (sequence summary) reports. Reports include headers, footers, pagination, logos, result tables, graphics and statistics.
Description of reporting capabilities	• WYSIWYG (report preview in Internet Explorer). The report template editor is HTML based • Full control of format attributes (layout, fonts, colors) • Automatic pagination • Headers and footers • Reports can be printed in 'Portrait' and 'Landscape'. • Chromatograms can be printed separately. (full page) • Result files can be printed separately from chromatograms. • Chromatograms and results can be combined on the same page. • The system can produce summary tables per analyte • Result reports include integration codes per peak • Peak markers are shown on the screen and in the report. • Peak names and retention times can be added to the chromatogram. • Date and time of printout is reported. • Date and time of processing or reprocessing is reported • Date and time of acquisition is reported • The scaling of a chromatogram in a report is user definable.
Data Archiving	
Description of Cerity data archiving capabilities	• The built-in archive/restore utility can be used to exchange electronic records (accurate and complete copies) as well as to restore and replay data throughout the record retention period. • Easy transfer of electronic records to other disks or media for long-term storage and to free up database space • Complete audit-trail of all archiving and delete operations. • Data selection is performed using an archive query wizard. • XML-based archive catalog allows for interface to archive management tools

Description of measures to ensure data integrity of archived data	• In order to maintain data integrity, Cerity archives related records in one consistent archive. • By design, the system prevents archiving incomplete information (e.g. an individual injection from sequence, or injection results without audit trail or method information). • If archived data was deleted from online storage, it needs to be reloaded to be accessed by the system.
Support of multi-tiered archiving technology	Requires 3rd party tool e.g., active data on hard drive, older data on slower optical magneto-optical disks, jukeboxes.

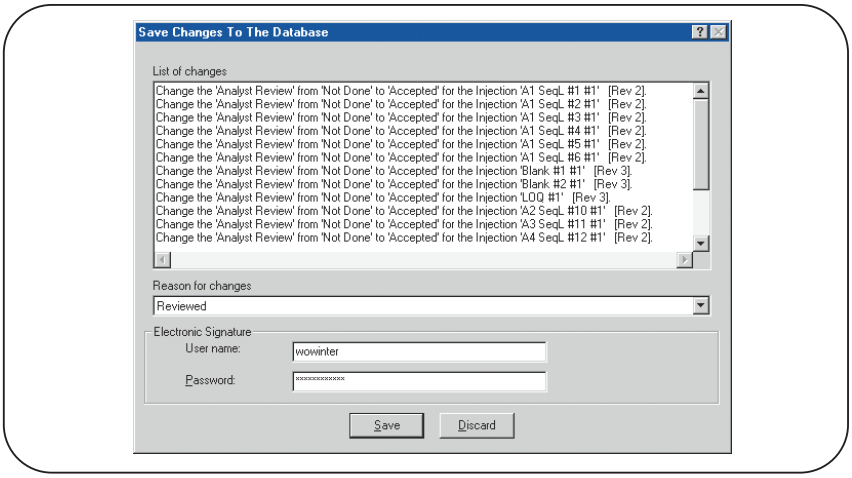


Figure 8
Audit trail and electronic signature for results sign-off

Where are electronic signatures used in the system? What infor-ma-tion is stored by the system for each use?	Configurable, depending on the organization's workflow. Includes, but is not limited to, method changes, adding/changing user permissions, result approval.
Are experiments and/or reports reviewed and approved in the system?	Yes. The information can be retrieved and inspected in electronic form as well as on paper for investigations or regulatory inspections.
What features does the system provide to administer user accounts?	Cerity users must be authenticated Windows users. The Cerity system administration console is based on the Microsoft Management Console (MMC) and is used to set the Cerity specific permissions.
Can the system support password aging?	Yes (reuses password policies defined on the operating system level).
Can the system support disabling / re-enabling user accounts?	Yes, by directly reusing the account policy defined in the Windows operating system.
Can the system support account lockouts after a defined number of failed attempts to log-in?	Yes, see above.
How are failed login attempts recorded by the system? How does the system administrator gain access to information about failed login attempts? How are other security problems identified, recorded and accessed by the system administrator?	Standard Windows security, event log and password policies.

Procedures and Controls for Closed Systems			
	Question	**Y/N/NA***	**Comments**
11.10(a)	Is the system validated?	Y	The software development is following the software life-cycle and quality management system of Agilent Technologies Lifescience and Chemical Analysis Group. Full installation qualification (IQ) and operational qualification (OQ) services available for the software as well as the instrumentation controlled by the system. *The product was designed to fulfill the validation requirements of the users of this product according to current regulations and quality standards including, but not limited to, 21 CFR 210 (Good Manufacturing Practice for Drugs), 21 CFR 211 (current Good Manufacturing Practice for finished pharmaceuticals), 21 CFR 58 (Good Laboratory Practice), 21 CFR Part 11 (Electronic Records and Signatures).*
11.10(a)	Is it possible to discern invalid or altered records?	Y	The data managed by the system is under strict access control, revisioning and automatic audit trail. The implementation ensures that alterations to records by authorized individuals result in a new revision of the respective record along with a detailed audit trail. Software operational qualification protocols and database integrity check utilities allow detecting corrupted data (e.g. due to a technical failure of a computer hardware component).
11.10(b)	Is the system capable of producing accurate and complete copies of electronic records on paper?	Y	Accurate and complete copies of electronic records are created and handled by the Cerity archive/restore utility included in the standard product In addition, the Cerity system provides an HTML based report editor that has the capability to render (visualize) the complete data records managed by the system.
11.10(b)	Is the system capable of producing accurate and complete copies of records in electronic form for inspection, review, and copying by the FDA?	Y	Data can be reviewed online in the query-based "Sample", "Instrument", "Method" and "Results Review" views. Navigation through hierarchical data is done using a treeview (similar to Windows Explorer). The Cerity archive/restore utility is designed to create accurate and complete copies of electronic records by maintaining complete referential integrity within the archive.
11.10(c)	Are the records readily retrievable throughout their retention period?	Y	The system manages all records under strict protection and revision control. Data is accessible directly from the user interface through predefined and customer definable selection criteria (queries). The system implements technical controls so data must be archived before an authorized system administrator can remove it from the online database.
11.10(d)	Is system access limited to authorized individuals?	Y	The system requires mandatory login. The system administrator grants user rights (capabilities) to individual users and groups of users. The system checks the user's capabilities prior to executing each task. The system's security implementation uses a combination of operating system (Windows 2000/Windows XP) security/password policies and application specific access controls.
11.10(e)	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?	Y	The system keeps a detailed, human-readable audit trail ("logbook"), which is automatically maintained independently from operators. The audit trail documents every time a record is created, modified or destroyed. Options for electronic sign-off on system tasks, configurable and mandatory audit comments as well as system checks for electronic results review and approval can be enabled using the optional Cerity GMP module (Agilent P/NG4030AA).

***Y=Yes, N=No, NA=Not Applicable**

	Question	Y/N/NA*	Comments
11.10(e)	Upon making a change to an electronic record, is previously recorded information still available (i.e., not obscured by the change)?	Y	The system implements strict revision control of its records. No previous entry is ever overwritten.
11.10(e)	Is an electronic record's audit trail retrievable throughout the record's retention period?	Y	The audit trail cannot be separated from the original record. The Cerity archive/restore utility maintains complete referential integrity of the record and archives the record along with its associated metadata and audit trail information.
11.10(e)	Is the audit trail available for review and copying by the FDA?	Y	The Cerity audit trail can be reviewed online (e.g. In results review) and can also be included in printed reports.
11.10(f)	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)?	Y	Operational checks: The system implements technical controls that ensure the permitted sequence of steps. Examples: The system enforces the approval-rejection cycle of results data by the person who generated the data (analyst review), by a 2nd individual (peer review) and final sign-off (final approval). The system's archive-delete cycle requires data to be archived prior to deletion.
11.10(g)	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?	Y	Authority checks: For every transaction, the security services determine whether the currently logged on user has the appropriate authorization based on the access permissions configured for this user or user group
11.10(h)	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 instruction 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).	Y	Device checks: The system performs input verification for data entry fields. Invalid fields are marked red. Agilent instruments automatically detect and record serial numbers and firmware versions. The system stores the hostname of the originating client PC when an electronic record is created or modified. For the 1100 HPLC, the system supports the use of column identifications tags that allow to trace and record analytical column information (e.g. batch number, number of injections, dimensions etc.)
11.10(i)	Is there documented training, including on the job training for system users, developers, IT support staff?	NA	Appropriate user and administrator trainings are available from Agilent Technologies. Customized trainings are available on request. Additional procedural controls are required."
11.10(j)	Is there a written policy that makes individuals fully accountable and responsible for actions initiated under their electronic signatures?	NA	This needs to be addressed by procedural controls in the user's environment.

***Y=Yes, N=No, NA=Not Applicable**

	Question	Y/N/NA*	Comments
11.10(k)	Is the distribution of, access to, and use of systems operation and maintenance documentation controlled?	NA	This needs to be addressed by procedural controls in the user's environment.
11.10(k)	Is there a formal change control procedure for system documentation that maintains a time sequenced audit trail for those changes made by the pharmaceutical organization?	NA	This needs to be addressed by procedural controls in the user's environment.

Additional Procedures and Controls for Open Systems

	Question	Y/N/NA*	Comments
11.30	Is data encrypted?	N	Not applicable.
11.30	Are digital signatures used?	N	Not applicable.

Signed Electronic Records

	Question	Y/N/NA*	Comments
11.50 (a) 11.30	Does signed electronic records contain the following related information?	Y	See detailed comments below.
	• The printed name of the signer	Y	System shows the printed name of the signer,date/time (local time and timezone information)
	• The date and time of signing	Y	See previous item
	• The meaning of the signing (such as approval, review, responsibility)	Y	The meaning of the signature is captured in the context of the function currently executed (e.g. peer review/approval) or through a mandatory comment.
11.50 (b)	Is the above information shown on displayed and printed copies of the electronic record?	Y	Signatures become part of the original record. Changes result in new revisions of records and previous entries are never overwritten. The information is available online and on printed reports.
11.70	Are signatures linked to their respective electronic records to ensure that they cannot be cut, copied, or otherwise transferred by ordinary means for the purpose of falsification?	Y	The signature information becomes part of the original record according to the Cerity database schema. Changes result in new revisions of records and previous entries are never overwritten. In addition, audit trail and e-sig are part of the archived/restored records

Electronic Signatures (General)

	Question	Y/N/NA*	Comments
11.100(a)	Are electronic signatures unique to an individual?	Y	The Cerity security implementation is based on operating system security. This allows to directly reuse the user account system defined by the user's IT operation along with the corresponding security and password policies developed and controlled by the user's organization.
11.100(a)	Are electronic signatures ever reused by, or reassigned to, anyone else?	Y	The Cerity security implementation is based on operating system security and supports appropriate behavioral controls of the user's organization. For instance, the operating system user account must be disabled but not reassigned to someone else when the respective individual leaves the organization
11.100(b)	Is the identity of an individual verified before an electronic signature is allocated?	Y	This must be governed by appropriate company policies.

***Y=Yes, N=No, NA=Not Applicable**

Electronic Signatures (Non-biometric)			
	Question	**Y/N/NA***	**Comments**
11.200(a)(1)(i)	Is the signature made up of at least two components, such as an identification code and password, or an id card and password?	Y	The Cerity system uses operating system security. Login to the Cerity system and electronic signatures require the user ID and password.
11.200(a)(1)(ii)	When several signings are made during a continuous session, is the password executed at each signing? (Note: both components must be executed at the first signing of a session).	Y	Signing a record always requires entering the user-id and password of that user.
11.200(a)(1)(iii)	If signings are not done in a continuous session, are both components of the electronic signature executed with each signing?	Y	A configurable inactivity timeout prevents impersonation after a defined period without user activity. The currently logged on user must re-enter user ID and password to unblock the system.
11.200(a)(2)	Are non-biometric signatures only used by their genuine owners?	Y	Customer policy has to define, implement and maintain a suitable password policy. Cerity uses Windows security system, allowing reuses of the password policies defined in Windows.
11.200(a)(3)	Would an attempt to falsify an electronic signature require the collaboration of at least two individuals?	Y	Yes, but requires appropriate account and password handling policies in the user's organization and IT environment.

For Tokens, Cards, and other Devices Bearing or Generating Identification Code or Password Information:			
	Question	**Y/N/NA***	**Comments**
11.300(c)	Is there a loss management procedure to be followed if a device is lost or stolen?	NA	This needs to be addressed by procedural controls in the user's environment.
11.300(c)	Is there a procedure for electronically disabling a device if it is lost, stolen, or potentially compromised?	NA	This needs to be addressed by procedural controls in the user's environment.
11.300(c)	Are there controls over the issuance of temporary and permanent replacements?	NA	This needs to be addressed by procedural controls in the user's environment.
11.300(e)	Is there initial and periodic testing of tokens and cards?	NA	This needs to be addressed by procedural controls in the user's environment.
11.300(e)	Does this testing check that there have been no unauthorized alterations?	NA	This needs to be addressed by procedural controls in the user's environment.

Electronic Signatures (Biometric)			
	Question	**Y/N/NA***	**Comments**
11.200(b)	Has it been shown that biometric electronic signatures can be used only by their genuine owner?	NA	Not applicable. Cerity for Pharmaceutical QA/QC revision A.02.xx is not delivered with biometric ID devices.

***Y=Yes, N=No, NA=Not Applicable**

Controls for Identification Codes and Passwords			
	Question	**Y/N/NA***	**Comments**
11.300(a)	Are controls in place to maintain the uniqueness of each combined identification code and password, such that no individual can have the same combination of identification code and password?	Y	Cerity uses the account system, security and password policies defined for the operating system. Therefore, this requires appropriate account and password handling policies in the user's organization and IT environment.
11.300(b)	Are procedures in place to ensure that the validity of identification codes is periodically checked?	Y	Yes, see 11.300(a)
11.300(b)	Do passwords periodically expire and need to be revised?	Y	Yes, see 11.300(a)
11.300(c)	Is there a procedure for electronically disabling an identification code or password if it is potentially compromised or lost?	Y	Yes, see 11.300(a)
11.300(d)	Is there a procedure for detecting attempts at unauthorized use and for informing security?	Y	Yes, see 11.300(a). The Cerity security implementation uses the operating system event viewer to log security events. This requires appropriate configuration of the operating system's event logging.
11.300(d)	Is there a procedure for reporting repeated or serious attempts at unauthorized use to management?	Y	Yes, see 11.300(a)
			***Y=Yes, N=No, NA=Not Applicable**

Warranty and Support Contracts	**Please contact your local support sales representative.**
Warranty Period	Varies by country and can be from 1-3 years.
Extended Warranty	Available.
Software telephone support	Available.
Software materials subscription	Available.
Software status bulletins	Available from www.agilent.com/chem/nds (requires valid software license number)

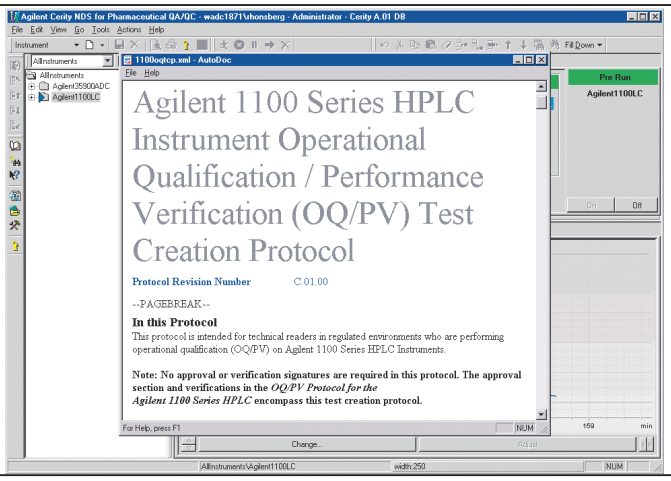


Figure 9
Computer based protocol for OQ/PV on an Agilent 1100 Series HPLC system

Services	Please contact your local NDS sales representative.
Standard Services	Installation, Familiarization, Education
Available Standard Courses	H2296A – Cerity Networked Data System Basic Operation (Full Access Users) 1 day H2297A – Cerity Networked Data System Advanced Operation (Full Access Users) 2 day H2298A – Cerity Networked Data System Application Administration 1 day H2295A – Cerity Networked Data System Routine Operation 1 day
Personalized Education Services	Customized education courses are available and can be delivered at a central Agilent location or on-site.
Qualification Services for NDS software	Computer-based installation qualification (IQ) Computer-based operation qualification (OQ/PV) Delivered by Agilent customer engineers or a certified support provider.
Qualification Services for chromatography equipment	Computer-based installation qualification (IQ) Computer-based operation qualification (OQ/PV) Delivered by Agilent customer engineers or certified support provider.
Customization Services	Available. Delivered through Agilent's Project Services Organization. Please contact your local NDS sales representative.
Consulting Services	Available. Delivered through Agilent's Project Services Organization.
Project Management Services	Available. Project management according to development lifecycle. Services comprise specification, design, implementation, deployment, validation and support. Delivered through Agilent's Project Services Organization.
Declaration of System Validation	Included with the shipment kit
Audit reports	The quality management system of Agilent Technologies and the lifecycle documentation for Cerity for Pharmaceutical QA/QC has been audited by independent inspectors according to PDA Technical Report #32. The audit report is available to subscribers from the audit repository center (ARC) *www.auditcenter.com*

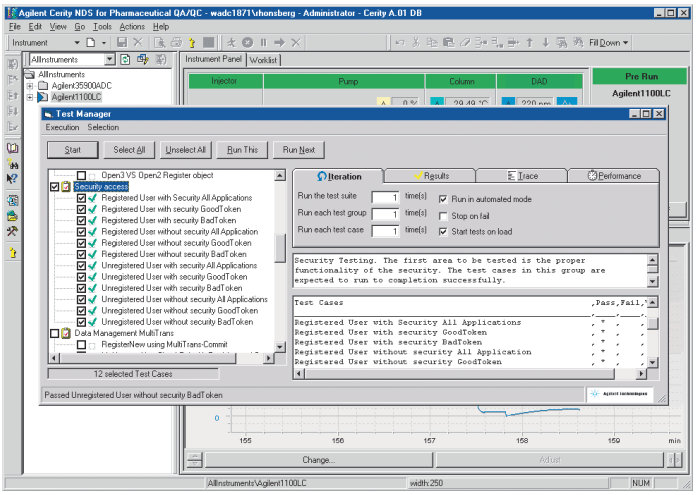


Figure 10
The software qualification protocols are based on the Cerity TestManager, an automated regression test utility

Figure 11
The audit report is available to subscribers from the audit repository center (ARC) www.auditcenter.com

www.agilent.com/chem/nds

Published July 1, 2003
Publication Number 5988-9763EN

Agilent Technologies