



支持 21 CFR Part 11 和附录 11 的法规要求：Agilent ICP Expert 软件和 SDA/SCM

白皮书



概述

美国联邦法规 21 章第 11 款（通常称为 21 CFR Part 11）是专门针对美国境内食品和药品的监管法规，其中包括了存储和保护电子记录、应用电子签名的美国联邦指南。在欧盟附录 11 中定义了同等类型的欧盟指南。

这些法规旨在确保电子记录的安全性、完整性和可追溯性，包括方法信息、数据、分析报告和其他与分析仪器操作有关的记录（如日常性能检查）。

安捷伦的 5110 ICP-OES 仪器由 ICP Expert 软件进行控制。Agilent ICP Expert (7.X 版及更高版本) 将安捷伦的另外两款软件产品（光谱配置管理器 (SCM) 和光谱数据库管理器 (SDA)）相结合，提供了支持 21 CFR Part 11 和附录 11 法规要求所需的功能。



Agilent Technologies

本文档对 21 CFR Part 11 指南的各章节进行了研究，并就使用安捷伦 ICP-OES 产品提出了推荐方法。文中还讨论了用于管理电子记录的其他常用功能。

将 Agilent ICP Expert 7.X 与 SCM/SDA 结合使用，为用户满足封闭系统的法规认证要求提供了支持框架。该系统能够对记录进行完整而准确的存储和恢复，并提供对用户帐户、密码和用户仪器软件中执行各种功能的权限进行管理控制的功能。

该系统将软件的所有用户与唯一的用户标识和密码组合相关联，在用户输入用户标识和密码组合并由系统进行验证后，方可允许用户访问仪器软件。通过执行电子签名功能进一步增强安全性，该功能要求用户对方法更改或仪器软件中采取的其他动作进行签署。所有这些更改以及进行更改的用户详细信息都记录在与用户无关、不可更改、带时间戳的审核追踪中，与受到更改的工作表永久关联。

安全设置可由系统管理员在安装时进行定制，以确保该设置满足组织操作规程和安全指南的任何特定要求。可定制的设置包括针对特定用户和组的仪器软件功能访问权限、用户密码长度、历史要求以及分析数据存储位置。通过这种方式可管理多个项目，并确保每个项目的用户、权限组和采集的分析数据在系统单次安装中的独立性和安全性。

《安捷伦光谱配置管理器 (SCM) 软件》文档中描述了系统设计和配置选项的详细信息：安装媒体中提供了《21 CFR Part 11 合规性》手册（部件号 G9292-90031）。关于已安装情景的更多信息，请参见“适用于 21 CFR Part 11 环境的软件安装说明”（部件号 G9292-90049）。除软件提供的说明之外，安捷伦在产品安装过程中为系统用户提供了基本的现场培训，以帮助其过渡至 21 CFR Part 11 法规认证。提供针对管理员和用户的培训课程。

安捷伦 ICP-OES 系统法规认证

在制药行业中，符合法规是分析实验室运营的重中之重。

与分析仪器有关的四项合规性内容是：

- 分析仪器及其软件的设计确认 (DQ)、生产质量控制、生命周期管理和记录、安装和操作确认 (IQ/OQ)
- 控制用户对工作站的访问以进行仪器控制和数据处理（通过密码保护方式限制用户登录访问）
- 电子记录安全性、完整性和可追溯性（安全存储、文件版本控制、审核追踪、电子签名、存档/检索）
- 系统操作控制、性能验证 (PQ)、对实验室及其相关设备的物理访问、标准操作规程、培训和记录

设计确认

法规监管实验室必须确保他们所用的设备是按照合格的质量流程进行设计、制造、测试、安装和认证的。对于仪器软件而言，这意味着仪器制造商须能够提供产品验证声明，确认其产品满足用户的 21 CFR 58（药物非临床研究质量管理规范）、21 CFR 210（药品生产质量管理规范）或 21 CFR 211（现行药物成品生产质量管理规范）认证要求。欧洲的 ISO 标准和国际协调会议 (ICH) 指南 Q8、Q9 和 Q10 提出了同等的 GxP 要求。安捷伦 ICP-OES ICP Expert 软件的产品验证声明示例见图 1。



图 1. 产品验证声明（左）示例和 IQ/OQ 确认报告封面页示例

安装和操作确认 (IQ/OQ)

产品交付至用户实验室之后，应马上对其进行进一步的确认检查，以确保产品符合规定的条款，并且系统的软硬件按照制造商的预期设计运行。

这些服务通常由制造商提供，被称为安装确认 (IQ) 和操作确认 (OQ)。应对仪器系统硬件及其操作所需的所有软件组件提供 IQ/OQ 服务。

ICP-OES 硬件和软件的 IQ/OQ 文件示例可参见图 1。

性能文档

用户组织的负责人员必须制定适当的实验室访问控制措施，确保预期方法的分析性能得到验证，并且书面记录例行操作规程。

设备安装、确认完毕后，通常应选用常规测量样品，按照特定的方法对设备进行分析检查（称为系统适用性测试，SST）。SST 确认系统性能满足实验室的特定分析要求。

需要通过标准操作规程根据 USP <232> 和 ICH Q3D 得到药物检测的完整解决方案，并需要创建这些标准操作规程。安捷伦手册可帮助用户整理 SOP。也可提供其他相关的产品和服务，例如样品前处理设备和认证校准标样，从而基于工作流程，对新型分析设备进行端到端的设置。

用户访问和电子记录

软件包通常控制和监控对工作站的访问，并提供安全的集成系统以处理实验室活动中生成的数据及其他电子记录。

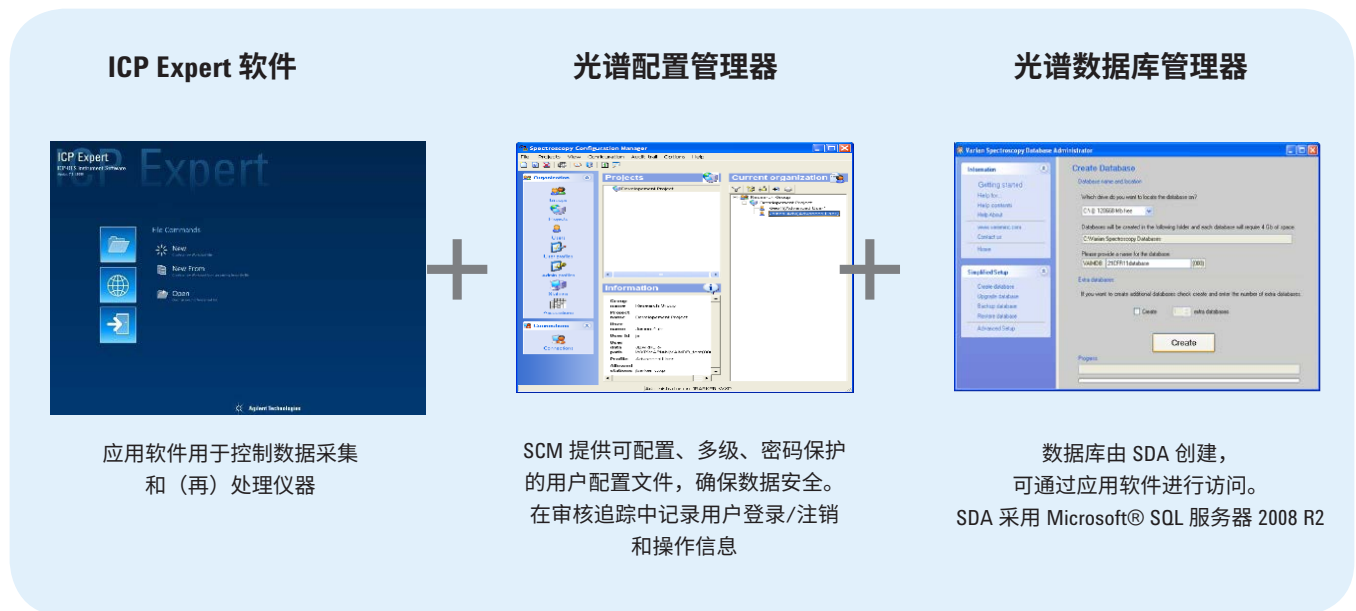
ICP Expert 的光谱配置管理器 (SCM) 以及光谱数据库管理器 (SDA) 可对这些功能提供支持。

配备 SCM 和 SDA 的 ICP Expert

为安捷伦 ICP-OES 仪器提供合规操作的软件组件如下图 2 所示。软件有多种安装情景，包括简单安装（所有软件组件安装于仪器控制 PC 上）以及网

络服务器上的各种分布式安装*。文档编号 G9292-90049 提供了有关推荐安装情景的更多信息。

* 已在特定服务器上进行了测试。有关支持分布式安装情景的服务器的更多信息，请参见《安捷伦光谱配置管理器系统要求》（文档编号 G9292-90047）



使用安捷伦 ICP-OES 软件满足 21 CFR Part 11 法规要求

下表描述了配备 SCM 和 SDA 的 Agilent ICP Expert 7.X 的特性和功能如何帮助实验室符合 21 CFR Part 11 的法规要求。

Part 11 的章节或其他内容	要求	是/否	如果选择是，具体说明如何满足要求；如果选择否，对用户有何建议？
验证			
11.10 (a)	质量管理体系支持系统验证。对系统进行验证，以确保准确性、可靠性、一致的预期性能，及识别无效或变更记录的能力。	是	为确保始终如一的产品质量，安捷伦根据完善的“产品周期”理念开发其产品，即用于软件和硬件开发的阶段审查流程。该流程要求系统在发布前经历评估流程，以确保软件特性和功能实现一致和预期的性能。 安捷伦提供了实施数据处理系统所需的完全合格的系统以及所有必需服务，以满足 FDA 关于 21CFR Part 11 的要求。每个软件副本均提供有验证证书。采用安全算法将 ICP Expert 软件生成的电子记录保存为一种受保护的专有格式。如果该记录通过其他应用程序进行了更改，那么在尝试读取记录时系统将检测到相应更改。
记录的准确副本以及安全保存和检索			
11.10 (b)	能够以便于阅读并且适合由 FDA 进行检验、审核和复制的电子形式生成准确完整的记录副本。	是	系统能够生成所有记录的准确完整副本。具体而言，ICP Expert 软件生成的所有方法和数据文件均以原始格式的完整文件保存在 SDA 数据库中。方法和数据文件包含电子记录、数据、方法审核追踪、操作人员身份以及电子签名，可随时使用客户端 PC 中的 ICP Expert 软件载入，这些文件可作为原始数据副本供 FDA 进行审核或检查。“已打印”记录可追溯至原始电子文件。
11.10 (c)	保护记录，使其能够在整个记录保存期内支持准确及时的检索。	是	ICP Expert 软件生成的记录保存在 SDA 数据库中。记录在保存后得到了保护，避免被修改或删除。SCM/SDA 的独特设计使 ICP Expert 生成的所有结果、数据或方法信息可自动保存在 SDA 数据库中。SDA 数据库中保存的数据位于受保护的位置或存档处。系统管理员应该根据公司级别的安全策略制定并实行额外程序控制措施，以管理归档、服务器维护、客户端计算机访问和密码策略管理等实践活动。拥有应用程序适当访问权限的用户可随时检索记录。
授权访问系统、功能和数据			
11.10 (d)	系统访问仅限于经过授权的人员。	是	对系统的访问取决于用户输入的有效且唯一的用户标识和密码组合。用户凭据由系统管理员决定创建，并可由管理员随时更改或撤销。系统支持强制执行密码要求，例如长度、重复使用以前的密码和密码过期。所有登录尝试无论成功与否，都记录在系统审核追踪中。此外，系统支持向不同用户或用户组分配不同级别的应用程序权限，允许精确控制特定用户在软件内可以达到的控制级别。

电子审核追踪			
11.10 (e)	利用由计算机生成的带时间标记的安全审核追踪，以独立记录操作人员登录及其创建、修改或删除电子记录操作的日期和时间。记录更改不得掩盖之前记录的信息。	是	有关创建、删除或修改电子记录的所有操作均记录于由计算机生成的带时间戳的审核追踪中。该审核追踪列出已发生的所有修改、进行修改的用户身份、修改时间和修改理由（如有）。审核追踪的条目不受用户影响，无法修改或删除。ICP Expert 软件和 SCM 可提供单独的审核追踪。除之前的条目之外还记录了新的审核跟踪条目，而以前的条目始终对用户可见。
操作和设备校验			
11.10 (f)	在适当情况下，使用操作系统校验执行允许的步骤和事件序列。	是	在需要事件序列时，通过系统校验强制执行。以下是几个示例： <ul style="list-style-type: none"> • 如果 QA/QC 中仅使用许可方法，即可通过限制用户访问 SDA 数据库中保存的许可方法实现 • 在 ICP Expert 软件中，针对电子记录的强制执行事件序列体现在软件确保在允许数据采集和分析前所需设置和设备可用，或确保在关闭 ICP Expert 软件前保存了文件。系统中的所有事件在审核追踪中均按顺序排列且带有时间戳
11.10 (g)	通过授权检查确保仅有经授权的个人可使用系统、签署电子记录、访问操作或计算机系统输入或输出设备、更改记录或执行当前操作。	是	如果没有有效的用户 ID、密码和帐户，用户就无法访问 ICP Expert 或 SCM/SDA。只有成功登录系统，才能访问文件和通用软件功能、仪器软件功能或归档和批准功能。在应用程序启动以及每次无操作超时或手动退出后，用户必须通过有效的用户 ID、密码和帐户进行验证。通过分配至个人用户的权限来进一步限制软件中特定功能的用户访问。需要时可将这些权限合并至特定角色中。输入用户 ID 和密码后，系统将检查用户 ID、密码、群组和项目以及给出的密码是否有效，以及是否符合定义的帐户策略和密码设置。
11.10 (h)	使用设备（如终端）校验，以在适当情况下确定数据输入或操作指令的有效性。	是	仪器访问权限仅限于已配置的设备。系统能够识别仪器型号和序列号，并采用专有的二进制进行通信。分别将仪器型号、固件版本号和序列号从 ICP-OES 传输至 ICP Expert 软件中。仪器序列号记录在 ICP Expert 报告中，而该文件保存在 SDA 数据库中。必须执行软件认证以确保设备和软件运行正常。
11.10 (i)	确定开发、维护或使用电子记录/电子签名系统的人员具备执行其获分配任务的教育技能、培训技能和经验。	是	安捷伦员工的教育和就业经历记录经过验证，可在现场审计期间进行查阅。此外，安捷伦所有相关员工均参加了法规要求培训。由使用系统的组织负责确保使用该系统的人员具备执行其任务所需的教育、培训和经验。安捷伦在安装产品时会为系统用户提供基本的现场培训。提供针对管理员和用户的培训课程。
11.10 (j)	制定并遵守书面政策，约束个人对其电子签名下发起的操作负责，以防止伪造记录或签名。	不适用	实行电子签名的组织负责制定书面政策，用于确保负责签署文件的个人了解其电子签名与其亲笔签名具有同等约束力。
11.10 (k) (1)	对系统操作和维护文档的分配、访问和使用进行充分控制。	不适用	虽然系统用户和管理员可访问文档，但安装和使用系统的组织应负责对这份材料的保存和分发进行控制。
11.10 (k) (2)	使用修订和变更控制规程，以对记录时序开发和系统文档修改的审核追踪进行维护。	是	安捷伦的质量流程包含用于系统文档的正式书面修订和变更控制规程。保存的所有文档修订均有时间戳，并创建审核追踪。

开放系统的控制			
11.30	必须使用规程和控制措施保护电子记录从创建时刻到接收时刻的真实性、完整性及保密性。	不适用	系统为封闭系统。
11.30	应采取其他措施确保电子记录从创建时刻到接收时刻的保密性。	不适用	系统为封闭系统。
电子签名 — 签名形式			
11.50 (a)	签署的电子记录包含的签名相关信息，即能明确指明：实施签名时签名者的姓名印刷体、签名日期和时间，以及与签名相关的含义。	是	具有指定的特定批准权限的用户可对 ICP Expert 进行电子签署和批准。电子签名和批准形式包括： <ul style="list-style-type: none"> • 签署人全名以外的用户 ID • 签署人头衔或资料 • 执行签名的日期和时间 • 与签名有关的用户可配置意义 所有签名均保存在结果文件中，且不可更改。
11.5 (b)	这些项目形成电子记录中任何便于阅读形式的一部分。	是	电子签名将显示于 ICP Expert 结果报告中，不仅以电子形式显示，还可进行打印。
7. 签名/记录链接			
11.7	电子记录中执行的电子签名和手写签名应链接到其相应的电子记录，以确保签名无法通过常规手段删除、复制或转移，从而伪造电子记录。	是	在 ICP Expert 中，输入签名和批准时需要系统校验的用户 ID 和密码。电子签名无法在不同记录或文件间相互转移，包括始终与电子记录共同保存的应用程序审核追踪中的自动输入条目。
电子签名 — 一般要求			
11.100 (a)	每个电子签名应专属于一个用户，且不得再次使用或重新分配给其他用户。	是	ICP Expert 签名和批准工具使用两个不同的识别组件，即唯一的用户 ID 和密码。每位用户都需要唯一的有效用户身份和密码。
11.100 (b)	在组织建立、分配、认证或批准个人的电子签名或该电子签名的任何元素之前，该组织应验证个人的身份。	不适用	这是计划、实施和操作系统的组织的责任。这样一个验证规程是执行电子签名程序或将电子签名权限分配给个人之前设定的系统要求。
1.100 (c)	组织在使用前或使用是否已将其电子签名使用声明交付给 FDA？是否是以手写签名的纸质形式？是否可以提供其他认证或证明，表明特定电子签名与签署人的手写签名具有同等法律约束力？	不适用	公司负责在向 FDA 提交电子签名的文档前记录其使用电子签名的意向。此外必须制定培训计划以确保以电子形式签署文档的用户了解其电子签名的法律重要性。
电子签名组件和控制			
11.200 (a) (i)	电子签名必须至少采用用户 ID 和密码等两种不同的身份组件。	是	ICP Expert 签名和批准工具使用两个不同的识别组件，即唯一的用户 ID 和密码。每位用户都需要唯一的有效用户身份和密码。任何两位用户不得拥有相同的用户 ID/密码组合。
11.200 (a) (1) (i)	当个人在一个连续的受控系统访问期间执行一系列签署操作时，应使用所有电子签名组件执行第一个签名；后续执行的签署应至少使用一种仅可由个人执行，并专为个人使用而设计的电子签名组件。	是	当个人在单个受控访问期间签署一系列文件中的第一份文件时，用户必须按要求输入两个签名组件，即用户 ID 和密码。每次后续签署还要求用户输入两个签名组件。

11.200 (a) (1) (ii)	当个人在一个连续的受控系统访问期间执行一次或多次签署操作时，每次签署都应使用所有电子签名组件。	是	未在一次连续的受控系统访问期间执行的每次签署都需要所有签名组件。
11.200 (a) (2)	应采取合适的控制措施以确保只有真正所有者可以使用电子签名。	是	对配备 SCM/SDA 的 ICP Expert 软件进行配置后，管理员可向新帐户或忘记密码的用户分配初始密码，但需要用户在其首次登录时更改该密码。这样，仅有相应个人掌握用户 ID 和密码组合。任何两位用户不得拥有相同的用户 ID/密码组合。
11.200 (a) (3)	通过管理和执行电子签名确保除真正所有者之外，任何人尝试使用个人电子签名时都要求两个或两个以上用户的合作。	是	对配备 SCM/SDA 的 ICP Expert 软件进行配置后，管理员可向新帐户或忘记密码的用户分配初始密码，但需要用户在其首次登录时更改该密码。这样，仅有相应个人掌握用户 ID 和密码组合。任何两位用户不得拥有相同的用户 ID/密码组合。运行该系统的组织负责强制执行这一政策。因此需要通过共享密码的积极合作实现对另一用户身份的使用。
11.200 (b)	基于生物识别的电子签名应旨在确保签名不为真正所有者之外的任何人使用。	不适用	当前系统不支持基于生物识别的签名。
身份识别码/密码的控制			
11.300 (a)	应采取合适的控制措施确保每个身份识别码和密码组合的唯一性，以避免出现两个用户拥有相同身份识别码和密码组合的情况。	是	配备 SCM/SDA 的 ICP Expert 要求用户通过其用户 ID 和密码进行验证。系统中的每位用户必须是唯一的，并被分配至唯一的用户帐户。每位用户都需要唯一的用户身份和密码。
11.300 (b)	采取合适的控制措施确保对发布的身份识别码和密码进行定期检查、找回或修改。	是	密码过期、历史和最小长度等密码管理的所有方面均可通过 SCM 指定。管理员可定义一个时间段，密码可在这一时间段内自动定期修改。这可以防止用户使用重复密码。
11.300 (c)	采取适当的丢失管理规程，通过电子方式禁用承载或生成身份识别码或密码信息的令牌、卡片及其他设备丢失、被盗、缺失或其他有潜在损害的情况。	不适用	当前系统不支持令牌或卡片等承载或生成身份识别码的设备。
11.300 (d)	利用合适的交互安全防护避免未经授权使用密码和/或身份识别码，检测并将未经授权尝试立即直接报告给系统安全部门和组织管理部门（在适当情况下）。	是	仅有用户知道其用户 ID 和密码。密码始终以星号形式显示，并以加密方式保存，因此即使管理员也无法看到。包括成功和不成功的登录尝试在内的所有系统访问尝试均记录于 SCM 系统审核追踪中。可通过配置 SCM 用户策略而使用户帐户在规定次数的失败访问尝试后被锁定。
11.300 (e)	对设备（例如承载或生成身份识别码或密码信息的令牌或卡片）进行适当的初始和定期测试，以确保其正常运行且没有未经授权的变更。	不适用	当前系统不支持令牌或卡片等承载或生成身份识别码的设备。

其他功能

除满足 21 CFR Part 11 直接规定的法规要求之外，Agilent ICP Expert 软件与 SCM/SDA 软件模块相结合，提供了许多其他特性和功能，使实验室能够更好地控制和信赖其分析数据的完整性。

要求	是否合规?	与 SCM/SDA 一起使用的 Agilent ICP Expert 7.X 的合规性
能够在网络 PC 上安装系统的管理组件，并与仪器控制软件的位置物理隔离。	是	系统允许 SCM/SDA 安装到与 ICP Expert 软件的位置物理隔离的计算机上，并通过 LAN 进行连接。该安装方法具有更高的数据安全级别，并使 ICP Expert 软件的多台仪器和安装能够在一套 SCM/SDA 下进行管理。
能够在批准后永久锁定数据集，使结果数据保持为只读状态，以免被编辑。	是	系统使 ICP Expert 工作表能够在结果获得批准和签署后永久锁定。这样可避免对结果数据进行任何编辑，并使工作表保持为获得批准时的状态。
能够备份和还原结果数据库，以防数据丢失。	是	系统使管理用户能够在需要时对结果数据库进行备份和还原。由使用系统的组织负责确保根据组织操作规程完成此操作，以防数据丢失。
支持将数据从旧版本或当前版本的系统迁移到未来版本。	是	系统以允许结果从旧版本系统迁移到新版本的格式存储数据，且不损失数据安全性或可追溯性。这也适用于与 ICP Expert 7.X 兼容的所有未来版本的系统。
系统必须避免未向审查人员提供明确指示，即在创建记录之前重新测试或终止测试。	是	在使用配备 SCM/SDA 的 ICP Expert 时，无法重复运行样品。这一软件组合锁定了这项功能。可以提前终止分析，但如果未保存现有数据，则无法提前终止。
必须将系统配置为在不活动期结束后自动注销或要求登录。	是	系统可以配置为在指定的不活动期结束后自动注销当前用户。在用户登录并通过身份验证之后，才可在系统内执行其他操作。
该系统易于扩展，以确保对采集的数据具有充足的存储容量。	是	针对系统内数据存储创建的 SQL 数据库的大小由用户决定。可创建多个数据库并将其链接至系统。允许的数据库大小仅受相关 PC 上可用存储空间的限制。

查找当地的安捷伦客户中心：
www.agilent.com/chem/contactus-cn

免费专线：
800-820-3278, 400-820-3278 (手机用户)

联系我们：
LSCA-China_800@agilent.com

在线询价：
www.agilent.com/chem/erfq-cn

www.agilent.com/chem/pharma

安捷伦对本资料可能存在的错误或由于提供、展示或使用本资料所造成的间接损失不承担任何责任。

本资料中的信息、说明和指标如有变更，恕不另行通知。

© 安捷伦科技（中国）有限公司，2017
2017年5月22日，中国出版
出版号：5991-8143CHCN