配备光谱配置管理器和光谱数据库管理器 (SCM/SDA) 的 Agilent MicroLab 软件

符合 21 CFR Part 11 法规要求

简介

美国联邦法规第 21 章第 11 款包含存储和保护电子记录及应用电子签名方面的美国联邦准则。实施这些准则的目的是为确保所有适用的电子记录可靠、真实并且保持高度完整性。

本技术简报描述了 Agilent MicroLab 软件（5.2 及更新版）的特性和功能，该软件配备用于实现数据管理和电子可追溯性的光谱配置管理器 (SCM) 和光谱数据库管理器 (SDA)，可帮助客户实施美国联邦法规第 21 章第 11 款的准则。

本文对 21 CFR Part 11 的各章节进行了研究，并就使用配备 SCM/SDA（1.0 或更高版本）的 Agilent MicroLab 软件提出了建议方法。该解决方案提供了系统访问、用户角色管理、数据转移和审核追踪方面的必需控制措施。此外，该方案不但确保了安全的记录保存，而且还具备数据存档功能。

配备 SCM/SDA 的 Agilent MicroLab 软件：21 CFR Part 11 合规性

使用配备 SCM/SDA 的 Agilent MicroLab 软件可为针对封闭系统的 21 CFR Part 11 规定的所有法规认证要求提供支持。特别是它能够确保：

- 准确完整地保留记录副本
- 管理用户帐户和密码
- 管理用户在应用程序中的访问权限
- 访问 MicroLab 前必须登录 SCM
- 电子签名功能
- 记录与用户无关的带时间戳的审核追踪中所捕获的更改

可在安装过程中对这些设置进行配置以符合特定的标准操作程序和安全指南。配置包括为单个用户或用户组提供应用软件和功能相应访问级别的定制化用户角色和权限。仅有专门的系统管理员可对安全配置进行更改。

《安捷伦光谱配置管理器 (SCM) 软件》手册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。关于已验证安装情景的更多信息，请参见“适用于 21 CFR Part 11 环境的 Pharma 软件安装说明”。

表 1. 关于配备 SCM/SDA 的 Agilent MicroLab 软件在封闭系统中运行的 21 CFR Part 11 适用章节（✓= 适用，N/A = 不适用）

MicroLab 在封闭系统中的可能情景	基于用户 ID 和密码的电子签名
11.1、11.2、11.3 范围、实施、定义	✓
11.10 封闭系统控制	✓
11.30 开放系统控制	N/A
11.50 签名形式	✓
11.70 签名记录链接	✓
11.100 电子签名一般要求	✓
11.200(a) 不基于生物识别的电子签名	✓
11.200(b) 基于生物识别的电子签名	N/A
11.300 (a), (b), (d) ID 代码和密码控制	✓
11.300 (e), (c) 令牌卡和其他 ID 设备	N/A

符合 21 CFR Part 11 的法规要求

下表描述配备 SCM 和 SDA 的 Agilent MicroLab 软件的特性和功能如何帮助实验室符合 21 CFR Part 11 的法规要求。

11.10	封闭系统控制		
章节	**问题**	**回答**	**配备 SCM/SDA 使用的 Agilent MicroLab 软件**
11.10(a)	系统是否经过验证以确保其能够识别无效或变更记录？ 哪些质量管理体系可支持系统验证？	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 MicroLab 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。
11.10(b)	系统能否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所有必需记录的准确完整副本？	是	系统能够生成所有记录的准确完整副本。 具体而言，MicroLab 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。 可随时使用客户端 PC 中的 MicroLab 软件载入包含电子记录、数据、方法审核追踪、操作人员身份以及电子签名的结果文件，该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)	记录在整个保存期是否得到了保护，以确保其准确并便于检索？	是	MicroLab 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 MicroLab 生成的所有结果、数据或方法文件可自动保存在 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。
11.10(d)	系统访问是否仅限于经过授权的人员？	是	系统访问取决于具备有效的授权用户身份和密码组合的用户。只有经系统管理员明确授权的用户才能访问系统。系统管理员还可决定 MicroLab 软件和 SCM/SDA 的访问级别和功能级别。相应人员可在 SCM 中管理 MicroLab 软件用户、角色和权限。 访问 MicroLab 软件需要同时输入两种身份组件：用户 ID 和密码。系统管理员根据内部标准操作程序对密码进行管理。系统支持密码过期功能，也可用于强制应用最小密码长度和组合。SCM 系统和安全审核追踪会对密码错误导致的登录失败等所有非法访问进行记录。此外，系统锁定可设置为手动锁定，或在一段规定时间内无人操作后自动注销。 所有文件和软件功能访问均通过分配至个人用户或用户组的特定权限和角色实现控制。MicroLab 权限可使授权的个人用户具有限定系统访问权限，并控制不同用户角色的访问级别。系统提供几个预定义的用户角色，系统管理员可向其中增加更多角色或对其进行定制化。可以根据访问限制启用或禁用应用程序中的菜单项、图形元素或视图。

11.10	封闭系统控制		
章节	**问题**	**回答**	**配备 SCM/SDA 使用的 Agilent MicroLab 软件**
11.10(e)	是否有由计算机生成的审核追踪，以独立记录操作人员登录及创建、修改或删除电子记录行为的日期和时间？	是	有关创建、修改或删除电子记录的所有行为均记录于由计算机生成的、带时间戳的审核追踪中。该审核追踪列出了所有修改、更改的日期和时间、用户 ID 以及更改原因（如适用）。审核追踪的条目不受用户影响，用户无法对其进行变更或删除。 MicroLab 软件和 SCM/SDA 确保所有数据与原始数据和结果共同得到保存。MicroLab 结果批处理文件包含与记录有关的所有方法、样品、数据以及应用程序审核追踪，以确保完全的数据完整性。 MicroLab 和 SCM/SDA 具有两类审核追踪： 1. SCM 审核追踪：SCM 审核追踪记录用户对系统的访问以及系统管理员在 SCM 内做出的任何更改。所记录的行为包括文件保存事件、应用程序登录或注销、电子签名以及对用户帐户或权限和档案的任何更改等项目。可随时对 SCM 审核追踪进行归档和检索 2. MicroLab 审核追踪：应用程序具有对结果和方法文件两方面的审核追踪。方法经过单独签名后才可使用。结果文件的审核追踪日志中包括了所有数据采集、分析和仪器/用户参数
11.10(e)	记录更改后，之前记录的审核追踪信息是否保持不变？	是	在 MicroLab 文件发生任何更改时，这一更改需要一个与电子记录唯一相关的新文件名。此外，审核追踪中的条目在生成后将自动与相关电子记录共同被保存。这些审核追踪条目既无法编辑也无法删除，除记录原始文件已被更改外，还记录时间、日期和操作人员。 通过在载入新方法或关闭应用程序等任何进一步操作前强制自动保存结果集到 SDA 数据库中，可对 MicroLab 生成的数据实现严格的修改控制。
11.10(e)	电子审核追踪的保存时间是否至少与其对象电子记录同样长，并可供机构进行审查和复制？	是	所有 MicroLab 审核追踪信息自动与相关电子记录共同保存，在保存期内均可访问。SCM 审核追踪中自动记录的登录事件等系统相关活动应永久链接至系统。 可在 MicroLab 软件中对审核追踪进行审查和打印。
11.10(f)	是否使用操作系统校验来执行步骤和事件的允许序列？	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： • 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 MicroLab 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 MicroLab 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)	是否有为确保仅有经授权的个人可使用系统、签署电子记录、访问操作系统/计算机系统输入或输出设备、更改记录或执行当前操作的授权检查？	是	如果没有有效的用户 ID、密码和帐户，用户就无法访问 MicroLab 或 SCM/SDA。只有成功登录系统，才能访问文件和通用软件功能、分光光度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	封闭系统控制		
章节	**问题**	**回答**	**配备 SCM/SDA 使用的 Agilent MicroLab 软件**
11.10(h)	是否使用设备校验在适当情况下确定数据来源或操作指令的有效性？	是	仪器访问权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分光光度计传输至 MicroLab 软件中。仪器序列号记录在 MicroLab 结果文件中，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)	开发、维护或使用电子记录和签名系统的人员是否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，所有安捷伦科技公司的相关员工均参加了法规要求培训。 要求 MicroLab 或 SCM/SDA 用户出示教育、培训和/或系统经验方面的记录。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)	是否已制定和遵循约束个人对其电子签名下发起的行为负责，以防止记录和签名伪造的书面政策？	N/A	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发、访问和使用是否有充分控制？	N/A	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)	是否有正式的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	安捷伦科技公司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，而且可以进行审核追踪。

11.30	开放系统的控制		
章节	**问题**	**回答**	**配备 SCM/SDA 的 Agilent MicroLab 软件**
11.30	是否有用于保护电子记录从创建时刻到接收时刻的真实性、完整性及保密性的规程和控制措施？	N/A	系统为封闭系统。
11.30	是否有用于确保电子记录从创建时刻到接收时刻保密性的其他措施？	N/A	系统为封闭系统。

11.50	签名形式		
章节	**问题**	**回答**	**配备 SCM/SDA 的 Agilent MicroLab 软件**
11.50(a)	已签署的电子记录是否包含明确说明下列内容的签署相关信息？ • 签署人的姓名 • 执行签名的日期和时间 • 与签名有关的意义	是	具有特定批准权限的用户可对 MicroLab 进行电子签署和批准。电子签名和批准形式包括： • 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。
11.50(b)	这些项目是否属于电子记录中任何便于阅读形式的一部分？	是	计算机生成的系统审核追踪会自动采集电子签名事件，且仅有具备相关访问权限以及有效用户身份和密码的用户才可签署电子签名。 电子签名将显示于 MicroLab 报告中，不仅以电子形式显示，还可进行打印。

11.70	签名/记录链接		
章节	**问题**	**回答**	**配备 SCM/SDA 的 Agilent MicroLab 软件**
11.70	电子签名是否链接到相应的电子记录，以确保签名无法以常规手段删除、复制或转移从而对其进行伪造？	是	在 MicroLab 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。

11.100	电子签名 — 一般要求		
章节	**问题**	**回答**	**配备 SCM/SDA 的 Agilent MicroLab 软件**
11.100(a)	每个电子签名是否专属于一个用户且无法再次使用或重新分配给其他用户？	是	MicroLab 签名和批准工具采用两种不同的身份组件：唯一的用户 ID 和密码。每个用户都需要唯一的有效用户身份和密码。
11.100(b)	组织在建立、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，是否会验证个人的身份？	N/A	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。
11.100(c)	组织在使用前或使用时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？	N/A	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。

11.200	电子签名组件和控制		
章节	**问题**	**回答**	**配备 SCM/SDA 的 Agilent MicroLab 软件**
11.200(a)(i)	电子签名是否至少采用了用户 ID 和密码等两种不同的身份组件？	是	MicroLab 签名和批准工具采用两种不同的身份组件：唯一的用户 ID 和密码。每个用户都需要唯一的有效用户 ID 和密码。任何两名用户不得拥有相同的用户 ID/密码组合。
11.200(a)(1)(i)	当个人在一次连续的受控系统访问期间执行一系列签署操作时，第一次执行的签署是否使用了所有电子签名组件？	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。
11.200(a)(1) (i)	当个人在一次连续的受控系统访问期间执行一系列签署操作时，后续执行的每次签署是否至少使用了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	在 MicroLab 签名应用程序中执行一系列连续电子签名的用户需要用户 ID 和密码两种组件。
11.200(a)(1) (ii)	当个人在多次不连续的受控系统访问期间执行一系列签署操作时，执行的每次签署是否都需要所有签名组件？	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)	是否有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 MicroLab 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。任何两名用户不得拥有相同的用户 ID/密码组合。
11.200(a)(3)	管理和执行电子签名的方式能否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 MicroLab 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。任何两名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非常规使用。
11.200(b)	基于生物识别的电子签名设计是否旨在确保签名仅为其真正所有者使用？	N/A	系统暂不支持基于生物识别的签名。

11.300	身份识别码/密码的控制		
章节	**问题**	**回答**	**配备 SCM/SDA 的 Agilent MicroLab 软件**
11.300(a)	是否有合适的控制措施可维持每个身份识别码和密码组合的唯一性，从而不会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 MicroLab 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。每个用户都需要唯一的有效用户身份和密码。
11.300(b)	是否有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)	对于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，是否有能够通过电子方式禁用的丢失管理规程？	N/A	系统暂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)	是否有合适的交互安全防护可防止未经授权使用密码和/或身份识别码？	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。
11.300(d)	是否有合适的交互安全防护可检测并将未经授权使用尝试立即紧急报告给系统安全部门和组织管理部门（适当情况下）？	是	可通过配置 SCM 用户策略而使用户帐户在规定次数的未经授权访问尝试后被锁定。 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。
11.300(e)	是否有合适控制措施对承载或生成身份识别码或密码信息的设备进行初始测试，以确保其正常运行且没有未经授权的变更？	N/A	系统暂不支持令牌或卡片等承载或生成身份识别码的设备。

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

如需了解更多关于安捷伦分子光谱产品的信息，请访问：
www.agilent.com/chem/molecularspectroscopy

如需了解更多关于安捷伦合规性软件的信息，请访问：
www.agilent.com

2015 年 7 月 15 日，中国出版
出版号：5991-6024CHCN

The Measure of Confidence

Agilent Technologies