BioPharm

生物制药
网络组件的确认和网络系统的验证

Ludwig Huber and Rory Budihandojo

为了符合 21 CFR 第 11 部分，你的网络系统需要与单个计算机一样的验证和确认步骤。但网络中还包括对共享服务器和多用户访问的要求。

本文中的斜体字由 www.biopharm-mag.com 上在线文章的“术语表”给出了定义。

Ludwig Huber *is worldwide product manager for pharmaceutical solutions at Agilent Technologies GmbH, PO Box 1280 D-76337, Waldbronn, Germany, +49.7243.602.209, fax +49.7243.602.501, ludwig_huber@agilent.com, www.agilent.com.* ***Rory Budihandojo*** *is head of R&D for IT quality and testing at the Centre of Excellence, GlaxoSmithKline, Collegeville, PA 19426.*

带有*集中*或*分布式数据库*的网络系统正在被制药行业广泛地使用。象所有计算机系统一样，必须对它们进行确认或验证，以保证它们满足使用的要求。虽然单机系统的验证已经被详细地说明了(1)，但许多公司仍不确定如何对网络和网络系统进行确认。FDA正越来越关注这样的系统，最近不断的警告信和检查报告就说明了这一点。为了符合规范的要求，需要对网络系统和应用程序进行验证，但验证对于商业也同样非常重要。电子批记录或实验室信息系统的数据丢失或研究报告的数据丢失对于公司和它的职员来说是一个灾难。由网络错误导致的产品延期交货也会造成很大的经济损失。我们将着重讨论网络组件(*交换机*、*集线器*、*路由器*和软件)的确认，以及网络系统的验证。我们假定读者已经对计算机验证和网络技术原理很熟悉。(参考文献1对于初学者来说是一本关于计算机验证的好书；有关网络技术和术语可以参见参考文献 2 和类似的书籍)。

Crosson, Campbell和Noonan对网络质量保证进行了阐述，他们认为网络可以被验证（因为它也是一种设备），并且通过文档控制（3）进行管理。Olthof在ECA会议（4）上发表文章讨论了*信息技术*（IT）的质量。在良好自动化生产规范(GAMP的)研讨会上有一个讨论组强调了质量保证对于IT基础设施的管理是非常重要的。这个组建议通过预先计划的确认过程，按照已有的标准，使IT基础设施符合规范要求。一旦符合要求，就应该使用文件化的标准规程和质量保证行为，来维护基础设施。程序的有效性应定期进行审计。

可以从以下一些网站上找到网络验证的最新发展状况：FDA的网站(www.fda.gov)，GAMP论坛(www.gamp.org)和PDA (www.pda.org)，以及一些私人网站，例如www.labcompliance.com 和 www.computervalidation.com。我们的目标是要为个人网络组件和网络系统的验证（作为支持网络的应用软件验证的一部分）提供切实可行的解决办法。

FDA 的希望

FDA正在检查网络系统，并已经发放了相关的警告信和483s，或检查报告。研究这些警告信和报告对于我们的工作是很有帮助的，因为我们可以从中了解FDA重点检查哪些项目以及其他厂家所犯的错误。下面的内容摘自于FDA网站上公开发布的警告信。

今年发布的两封有关网络方面的警告信包含了实验室信息管理系统和稳定性试验的相关内容。第二封警告信包含了有关数据库的内容。

网络程序缺乏足够的验证/或文件支持。例如：

- 自1985年起的生命期间，...软件进行了显著的变化和修改，但却没有对系统设计

文件进行维护或升级。这包括程序代码、功能/结构设计、图表、规格参数和与[这个程序有关]的其它程序的文本文件。

- 软件的验证文件没有进行详细的定义、升级，对于为满足特殊要求的操作而定制的系统，没有进行足够的控制。
- 验证文件没有包括完整的和最新的设计文件，没有完成布线/网络图纸来说明所有与...系统相连接的所有计算机和设备。
- QCU（质量控制部门）没有制订足够的规程来定义和控制计算机化的操作过程、设备验证、文件回顾和实验室操作（6）。

一个允许不同部门的人，包括生产、实验室和质量保证，访问的...计算机系统缺乏以下内容：

- 数据库的审计追踪功能，用以防止记录的丢失或删除。
- 缺乏相关文件来定义数据库、操作系统、本地文件和数据库的安全访问。

[...]

你们的答复中没有提供需要进行定义和控制的系统的回顾性验证，这应该作为整体配置管理的一部分（7）。

在2000年七月的FDA 483中引用了一个公司培训记录不完全的例子：

没有文件记录表明信息技术（IT）服务提供商的工作人员接受过包括CGMP和法规规定的书写规程的相关培训（8）。

FDA的警告信和检查报告一再强调要对升级进行控制，这篇文章对此进行了重点描述。在Labompliance的网站上可以找到有关计算机和网络内容的警告信的摘录和例子（9）。

什么需要验证

*网络*是连接若干台计算机和外部设备的系统。网络的主要目的是进行数据的传输并控制传输过程。不论数据是否储存在网络服务器上或其它地方，网络必须能够确保数据在传输过程中的完整性和安全性。可以通过控制和正确管理网络的访问，以及将数据安全的保存在网络上来确保数据的完整性和安全性。

计算机系统必须经过确认和认证来证明它们符合使用的要求。这意味着所有用于良好实验室操作规范、良好生产操作规范（加上其它的GXP）的系统（包括网络）都必须经过验证。21CFR第11部分详细说明了使用电子记录的哪些计算机系统需要符合规定：所有创建、修改、维护、归档、追溯或发布电子记录的系统（10）。为了确保符合规定，我们建议最好仔细分析FDA检查时所提的要求。如果文件或数据经过一台计算机或其它设备时有可能被修改，那么这台计算机或设备就要进行验证。

因此如果计算机是用于获得或评估测量系统的关键数据，或办公室的计算机需要产生报告给FDA，那验证就是很必要的。生成标准操作规程（sop）的文字处理系统同样需要验证，另外，运行这些程序的计算机通常与网络相连接。对所有生成和评估关键数据的计算机系统进行验证，除了可以符合规定外，还是一种良好的商业行为。

网络系统

图1显示了一个典型的*客户/服务器型*的网络系统，它的客户端在实验室，服务器则位于机房。机房同时也有*邮件服务器*。带有*数据系统应用软件*的实验室计算机使用*TCP/IP 协议*获得数据，并对内置的*局域网卡*进行仪器控制。客户端的应用软件用于数据评估。计算机通过*集线器*连接在服务器上。每一个服务器都使用带有定制应用程序的*关系型数据库*（例如Oracle数据库），定制程序一般用于数据管理；图表控制和统计；回顾、备份、归档和数据追溯；生成符合21CFR第11部分的电子签名。

其它经常在制药行业中使用的网络系统包括企业资产管理系统（EAM）、制造资源计划（MRP）、带有电子批记录功能的制造执行系统（MES）和电子文档管理系统（EDMS）。它们的安排可以和图1所示的一样；对于验证的要求也是一样的。

验证一个网络系统需要确认每一个组件（例如在每一台计算机上运行的应用程序）和系统的授权访问，同时也要确认在两台相关联计算机之间的数据

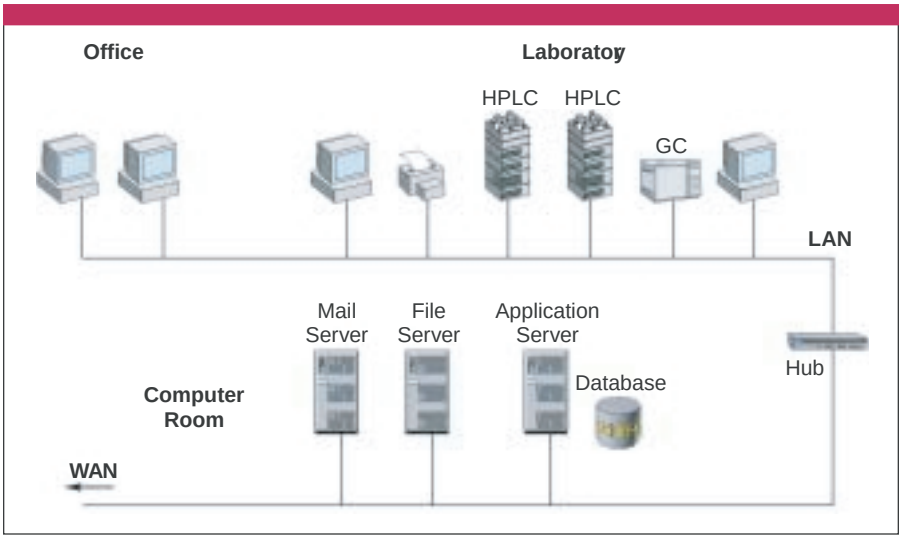

Figure 1. Example of client/server networked system (4)

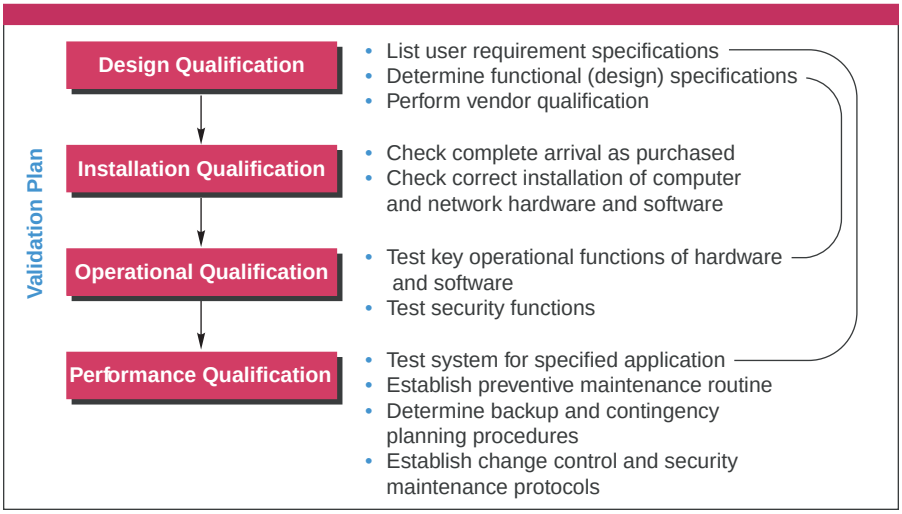

图 2. 网络系统的 4Q 确认模型

传输（也就是说在这两个组件的界面）。整个系统，包括网络本身，都需要通过在正常和最差情况下运行日常的应用软件，来进行验证，并确保系统和它相应的功能能符合先前的规定。

对于确认组件和整个系统的验证来说，定义*验证盒*是很重要的。验证盒的目的是将网络细分成子网，每个子网包含相应应用程序的网络组件。验证盒可以描述整个网络的哪一部分需要确认，哪一部分不需要。如图 1 所示的实验室数据系统的验证盒将包括实验室计算机、文件服务器、应用服务器和数据库。将网络确认工作集中到那些具有网络功能的组件，将会节约时间。

4Q 模型

网络系统的验证在原则上应遵循其它计算机的验证过程。对于单个计算机验证来说如果是重要的事项，那对于网络验证来说同样是重要的。网络验证活动应按照验证计划进行。如果其它计算机已经有了验证计划，那有关网络的验证应加到验证计划中。网络组件应该象其它设备一样进行安装和确认。

一个网络组件应该象其它设备一样进行安装和确认（例如，用于峰面积积分和计算的色谱软件功能）。典型的网络功能，例如安全访问和网络交易，应该被确认。因为网络系统的复杂性，一个具有交叉功能的队伍应该控制验证活动。对于网络验证，应该按照特定的步骤（例如生命周期模型）进行；例如，图 2 的 4Q 模型，它包括设计、安装、操作和运行认证。

设计认证（DQ）是第一步，它确保网络的设计符合使用者的要求。在这一阶段，应指明用户对每一种功能的要求。例如，一个用户可能要求，“网络应该具备安全访问功能”。为符合这样的要求，网络应具备如下功能，“当访问系统时，应该有输入用户 ID 和密码的地方”。在 DQ 阶段，应该对计算机系统供货商进行资格确认。

安装认证（IQ）是第二个阶段，用来检查所运来的设备就是要买的。然后安装网络组件并完成相应的文件。

操作认证（OQ）是第三步。要进行主要功能测试。测试时要遵循测试计划，并将测试结果与制订的标准相比较。

运行认证（PQ）是最后阶段，通过投入使用来测试整个系统。在进行 PQ 时将对指定的硬件、附件和软件使用样品设备进行全面分析。它还包括预防性维护，例如例行的磁盘维护和变更控制。

特殊要求

计算机网络系统与单机不同，它有一些特殊的地方，需要在验证中加以注意。单机系统包括一套硬件与软件。但网络与之不同，它是多样性的，通常包括很多不同的硬件，软件应用程序和通讯协议。其中一个的变化会影响其它的使用。

在网络系统中，布线设计与规格参数同软硬件一样重要，主要因为网络上的各部分也许相距很遥远。许多人和部门将网络作为普通资源使用，因此安全性非常重要。网络可以同时包括必须符合规范的组件和那些不符合规范的组件，而且不是所有的 IT 人都接受过 GXP 培训。

验证计划与队伍

规范并不要求主验证计划，但 FDA 检查员也许会要求对验证步骤进行说明。主验证计划对于这种说明是很有帮助的，而且这种计划对于单地址公司和多地址公司同样适用。主验证计划能确保验证在公司内持续和有效地实施。如果已经有了主验证计划，那么这个计划可以很容易地进行扩展来包括网络系统。我们建议先制订一个一般性计划，然后再加上网络部分。例如在术语表中加上网络名词解释。

网络技术指标应成为主计划的一部分（例如布线、安全、供货商资质考察）。它还应包括备份、应急计划、灾难恢复、变更控制、验证报告和归档等内容。计划还应包括名称约定，这将使在网络中识别组件和追踪*数据流*很容易。还要包括日常操作的模板作为持续实施的附录，对现有的 SOP 应制订参考。主计划是单个项目验证计划的良好基础。

验证队伍可以协调网络系统的验证活动。网络的复杂性需要不止一个有关定义、确认和变更控制（最重要的）方

面的专家。验证队伍应包括IT专业人员。他们能最好地描述系统会遇到什么样的问题以及个人网络组件如何影响其他人。

实验室人员应该成为验证队伍的一部分，来确保文件和控制符合规范和公司政策的要求。如果全部或部分的软件由自己开发，则还应该包含软件工程人员，否则要包括供货商代表。如果有必要，队伍还要包括咨询人员，他们对大型网络验证项目会起很大帮助。

技术指标类型

所有验证活动都应该从最重要的一步开始作起：技术指标设定。好的技术指标可以在整个验证活动中一直被使用。用户对于技术指标的设定要求一般说明了他们希望用网络作些什么。典型的要求一般包括共享、打印文件和了解有多少个用户能够在网络上工作。另一个要求是限制和授权访问系统。功能性技术指标则说明了网络或它的组件应该具有什么样的功能才能满足这些目标。

主验证计划要包括其它两种技术指标— 设计指标和环境指标。作为功能性技术指标的一部分，设计指标作为功能性指标的一部分详细说明了为满足特定功能的要求，而进行的计算机硬件、软件、连接器和布线的设计。环境技术指标详细说明了网络在什么样环境条件（例如温度或湿度）下工作。

当确定了网络技术指标，要确认可以回答如下问题：网络能够负担多大的数据流量，特别是在最大负荷和最坏的情况下？单个网络组件之间实际最远可以相隔多远？有多少个用户可以同时在网络上工作？如果服务器瘫痪，会有什么样的风险以及会造成多大的损害？多长时间进行备份和归档？网络在什么样的环境条件下工作？使用什么样的通讯协议（例如GPIB-IEEE或TCP/IP）？现有的工作站是否可以满足网络的要求，要进行更换或增加吗？

当进行技术指标设定的时候，上面的每一个问题和答案都是非常重要的。用户应仔细回答以上问题，验证队伍的成员应讨论每一个问题。

安装

网络安装步骤同其它计算机系统的安装相类似。检查运来的货物（计算机硬件、软件、网络硬件、电缆和操作说明书）是否就是所购买的。检查所有的设备和相关材料完好无损和干净。确认环境容忍度符合指定要求（包括温度、湿度、无线电频率和电磁干扰）。考察是否符合物理安全技术指标（例如带锁的硬件可以防止未授权人进入服务器的RAID系统）。

根据供货商的建议安装组件，对所有网络设置进行配置和文件化（例如路由器的设定）。对所有设备给予唯一编码：硬件、软件、电缆、固件和操作系统。同时记录下网络用软件和固件、以及硬件、软件和用于网络基础设施电缆的版本号。如果将版本号记录到数据库中或网络配置管理工具中，将会很容易进行追踪。

图纸创建系统设计图，并将其作为系统安装的一部分。这样的图纸对于网络或网络系统的安装是非常必要的，而且它们对于系统维护更重要。设计图纸应该和其它IQ文件保存在一起，同时还应包括施工图（例如组件位置和布线）以及逻辑图纸（例如TCP/IP方案和有多少组件相互连接）。在动态IP地址分配系统，图纸还应说明如何实现动态IP（包括IP地址的子网掩码）。图纸能使IT人员和检察员追踪数据传输过程，并确保数据的完整性和安全性。网络的变化很频繁，所以进行带文件版本号控制的图纸维护是很重要的。我们建议对规程进行定期复审（也许以季度为单位）。

测试

供货商不仅要在开发环境中进行测试，还应该在用户环境中进行测试，并将测试作为验收和/或OQ过程的一部分。在安装、变化和定期维护后，应对系统进行测试。当发生改变时，应该对变化的组件进行测试来考察它是否可以在网络中工作，同时还应该对其它组件进行测试因为它们也许会受到这种变化的影响。需要制订带有设定技术参数和验收标准的测试计划。测试计划在实施前应经过批准。

应定期检查关键功能。例如21 CFR第11部分所要求要进行认证的设备，以及网络交易的准确性。除了对所有计算机进行一般性测试外，还要对网络进行一些特殊测试。请参见“基于网络的特殊测试”的相关内容。

网络交易的准确性也要进行检查。应确认数据在客户计算机与服务器计算机之间安全传输。这应该作为OQ的一部分。但现在有这样的技术可以自动完成确认工作。它通过定期计算每一个文件的*校验和*和*散乱值*，并将这些数值附在文件中，在数据交易之后，重新计算这些值，并将其与先前附在文件中的值进行对比。这些步骤可以由软件自动完成，而不需要人工干预。软件应该自动记录和报告错误。*散乱算法*现在已经商品化，例如RSA（www.rsa.com）的MD5软件。如果可以正确应用校验和与散乱算法，计算可以执行得非常快，以至于对系统的操作无任何影响。

如果很多用户使用完全一样的硬件和软件配置，你也许会问是否有必要对

项目相关文件

必须定期回顾项目相关文件，如果有必要，要进行更新。在项目相关文件中要包括如下文件:

验收测试方案或仪器认证方案

备份要求

有计划的灾难恢复程序

安装认证文件

变更日志

维护过程

网络主要组件清单（例如那些对网络操作起关键作用的组件）

项目计划

报告摘要

测试、备份和应急计划的风险评估

系统和网络设计图（例如建筑平面图、拓扑图和布线图）

与计算机系统相关的培训记录

用户要求（功能、设计和环境技术指标）

供货商评估

每个用户都要单独测试。这个问题的答案应该基于风险评估：每一个用户特有的错误是否会影响产品质量？在大多数情况下，仅测试一定百分比用户带来的风险是可以接受的。

以上的大部分内容测试了网络系统本身或运行在网络上的应用软件（例如在两个或多个系统组件之间的交易）。对关键组件也可以进行测试，例如可以测试交换机的缓冲区以确保没有数据丢失。

数据备份和应急计划

应该制订数据备份和恢复的规程。通过风险评估来决定备份时间。对于关键数据或容易丢失的数据要提高备份频率。已经有商品化的硬件和软件来完成这项工作，但要对单个设备的备份和恢复进行验证。在一个服务器完全损坏的情况下，应该能够在没有数据丢失的情况下，将数据库恢复到另一个服务器上，这也应该进行验证。

网络系统有可能因为各种原因而瘫痪。设计不好的应用程序也许不能在网络上运行，单个组件也许会出现错误。当设计网络时，要回答如下问题：当一个或多个组件出现错误的时候，过程还要继续吗？这种情况将如何影响商业活动？错误会是什么样的？一旦网络恢复，如何恢复数据？对这些问题的回答将决定应急计划（如果一个或多个网络组件停止工作，可以确保网络正常工作）的紧迫性。这种计划对于法规和出于商业角度考虑都是非常重要的。

应急计划应该以风险评估作为开始：当数据丢失，损失会有多大？应急计划的花费与数据丢失造成的损失相比会如何？

经过验证的*冗余系统*可以帮助系统更有操作性。其它类型的网络操作计划可以包括热址使用。因为恢复网络操作所花的时间是关键性的问题，所以应该考虑在热址上运行的认证及类型；有时候运行全套的认证不太方便。在灾难发生之前应将计划进行演习，以确保在出现问题的时候可以安全地保存和恢复数据。

安全维护

网络经常变化，不论是硬件或软件或两者都是。对所有的变化应进行管理、控制和记入文件。在某些情况下花费很大精力进行再验证是必须的。在决定进行改变之前，你需要问自己几个问题：是否真的需要进行变化？要将收获与花费相比较。计算花费时不仅要包括购买的费用还要包括验证费用，也许后者会更贵。这些变化会怎样影响系统和它的组件？在变化之后需要对什么进行测试并记入文件？需要通知谁？

这些问题必须由验证小组来回答而不是由个人来回答。一位实验室的化验员不大可能知道将一个客户端加入到一个繁忙的网络中所产生的影响。但一个 IT 专家在得到化验员的通知后，会对新计算机产生的数据流进行很好的估计。

在每一次变化之后，要再认证网络组件，并将认证结果文件化。在变化之后，要对有关设备数据库进行更新并画图。对机房、计算机硬件、网络硬件的进入要进行管理，并且要有选择地定期检查任务和数据。当雇员进行工作调动时，要维护并更新他们相关的权限。

文件化

所有验证活动，包括网络系统和数据库的认证，验证计划和结果都要文件化。有两种类型的文件：说明每一个项目的特定项目文件和描述政　，主计划和过程的通用文件。模板能够促进验证的持续实施和使用。好的文件化对于解决问题是非常重要的。

通用文件应包括主验证计划和现有计算机验证的主计划以及添加和删除网络组件、连接到网络的步骤。控制网络安全包括物理和逻辑安全、密码策略和管理步骤；在多地址间的网络管理；配置管理；变更控制步骤（设备、硬件、软件、固件、电缆和连接），以及 GXP 规范要求的培训记录。

所有过程都应该每年定期回顾，以确认它们是按规定进行。对所有变化进行版本控制。项目相关的文件必须定期回顾，如有必要要更新。请参见“项

相关网络测试

启动和停止整个网络系统（将网络正确响应启动和停止的信息记入档案）。打开和关闭网络组件（例如集线器、路由器和交换机），将这些操作对网络的影响记录下来。

进行安全测试，例如用正确和不正确的密码登录。以系统管理员身份访问，确认系统管理员知道对于网络环境他们可以和不可以做什么。检查密码管理工作正常，例如在规定密码长度至少为六位的系统中，用四位密码进行检查。

确认任务解锁以及特定用户的自动超时可以正常工作。确认对任务和文件的访问许可，例如让一位具有回顾数据权限的操作员去修改数据，来考察系统是否按要求工作。检查网络的数据备份和恢复工作可以正常工作。

通过断开然后再接上某个网络组件制造网络错误，来确认系统如何处理故障并从故障中恢复。测试出错信息和其它相关的反应也是测试的一部分。

检查网络交易的审计追踪是否正确。确认数据可以在正常和高传输量的情况下正常传输。

检查单个软件和系统免受病毒感染。组建系统完整性反应小组，它的功能是在内部和外部断开的情况下，提供损失报告。

目相关的文件”清单来决定应包括什么内容。

实施

总而言之，网络组件的确认和网络系统的验证对于符合规范要求和出于商业角度考虑都是非常重要的。我们建议采取分步实施步骤。

按照计算机验证指南来做。最重要的是要按照确认和验证的生命周期，制订主计划，或在现有计算机验证的主计划中加入网络部分内容。组建验证项目小组。根据功能和设计规范来提出用户要求。

将每一个网络组件都作为一个设备对待，都要进行认证，但只认证那些运行应用程序的组件。安装组件并测试（认证）。将组件结合到网络中，并测试它们。通过运行完整的应用程序来验证网络系统。对于复杂的网络，不要测试每一样东西，要有选择性。使用风险评估。如果你有20个使用同样软件的相同用户，测试他们之中的两三个就足够了。

对于变更，评估是否真的需要每一个变更。评价它们是否有很好的商业价值值得实施。在你觉得进行变更后，要测试这种变更对其它组件的影响。不要假定在变更之后，其它组件还会象以前一样工作得很好。不要忘记在变更控制过程中，要继续认证工作。

制订备份、应急计划和灾难恢复计划。要建立良好的文件体系：SOP、模板、维护日志等等。对技术和操作以及法规内容对你的人员进行培训，包括IT人员。

参考文献

(1) L. Huber, *Validation of Computerized Analytical Instruments* (Interpharm Press, Inc., Buffalo Grove, IL, May 1995).

(2) N. Jenkins and S. Schatt, *Understanding Local Area Networks: Easy Introduction to Network Concepts and Products* (SAMS Publishing, Indianapolis, 1998).

(3) J.E. Crosson, M.W. Campbell, and T. Noonan, “Network Management in an FDA-Regulated Environment,” *PDA Journal* 53(6), 280–286 (1999).

(4) H. Olthof, “GXP Requirements for IT Infrastructure,” presented at the ECA conference: FDA 21 CFR Part 11 Compliance for Pharmaceutical Laboratories (European Compliance Academy, Copenhagen, Denmark), October 2000.

(5) IT Infrastructure Special Interest Group, *Quality Assurance* (GAMP, Tampa, FL, 2000), draft document.

(6) J.C. Famulare, Warning Letter #320-01-08 (Center for Drug Evaluation and Research, 11 January 2001). Available at www.fda.gov/foi/warning_letters/m5056n.pdf.

(7) J.C. Famulare, Warning Letter #320-01-07 (Center for Drug Evaluation and Research, 11 January 2001). Available at www.fda.gov/foi/warning_letters/m5057n.pdf.

(8) “FDA 483 Observations Related to IT” (Labcompliance, July 2000). Available at www.labcompliance.com/publications/lit-references.htm.

(9) “FDA 483 Inspectional Observations and Warning Letters Related to Computers” (Labcompliance web site). Available at www.labcompliance.com/computer/fda-observations.htm.

(10) *Code of Federal Regulations, Food and Drugs*, “Electronic Records; Electronic Signatures,” Title 21, Part 11 (U.S. Government Printing Office, Washington DC), issued March 2000. Also *Federal Register* 62(54), 13429–13466. Available at www.fda.gov/ora/compliance_ref/part11. ***BP***

出版号：5988-5104CHCN