Focus On Quality

Validation of Spectrometry Software

Part VIII – Understanding Change Control and its Importance in Maintaining a System's Validation Status

R.D. McDowall

One thing that is constant in analytical laboratories is change. Unfortunately, when we are dealing with a validated computerized system, almost all changes must be managed and controlled. Throughout this series of columns we have gotten to the point where we have validated our spectrometer and its software. You'll now be looking forward to getting your lab coat on and getting back to doing some real work — analyzing some samples and forgetting about validation. However, you can't forget about validation and waste all your hard effort. Unfortunately, many computer validations suffer this fate and consequently face an increasing regulatory risk.

After the operational release of the system comes the most difficult part of any computerized system validation — maintaining the validation status of the system throughout its whole operational life. Look at the some of the challenges that will be faced when dealing with maintaining the validation of a spectrometer (or any system); following are some of the types of changes that will affect an operational system:

- Software bugs will be found and the associated fixes installed.
- Application software, the operating system, and any software tools or middleware used by the system will be upgraded.
- Network improvements will be necessary, such as changes in hardware, cabling, routers, and switches to cope with increased traffic and volume (only applicable if your system is networked).
- Hardware changes likely will occur, such as workstations and any associated server upgrades or increases in memory and disk storage.
- New applications such as spreadsheets or laboratory information management systems (LIMS) will need to be integrated.
- Changes might occur to the use of the system due to work or organization reasons.
- Environmental changes might be implemented, such as moving or renovating laboratories.

All of these changes need to be controlled to maintain the validation status of the spectrometer and its computerized system.

In this installment of Focus on Quality, we'll discuss the major item that must be in place when your system becomes operational: change control. Your spectrometry software might not be free of bugs or features that could have an impact on the quality of your generated results. You'll need to know which version of software was operational and between which dates.

Closely associated with change control is configuration management; this is the identification and management of the defined components of your system. We'll look at both these concepts and see how they work in a regulated environment.

R.D. McDowall
is a visiting senior lecturer in the Department of Chemistry at the University of Surrey, principal of McDowall Consulting (Bromley, UK), and "Questions of Quality" column editor for *LCGC Europe, Spectroscopy's* sister magazine.
Address correspondence to him at 73 Murray Avenue, Bromley, Kent, BR1 3DJ, UK.

What Do the Regulators Want?

When I audit an operational computer system, I start with changes to the system during the period of time that the system has been running. Changes always occur, and because few systems remain in their initial configuration for long it is essential to track all modifications to a system. This reiterates the original purpose of many quality guidelines: being able to repeat conditions under which the work was originally done.

The key concern from an inspector's perspective is whether there is demonstrable control of these changes. In many cases change is uncontrolled. Let's look at what the inspectors want from their guidance documents and regulations.

There are references in both US FDA and European Union good manufacturing practice (GMP) regulations to the need to control changes to computerized systems (21 CFR 211.68 and Annex 11 respectively). However, the guidance documents themselves give the most information about change and what you need to do to control it.

The sidebar lists some of the items that an inspector could look at during a visit to your laboratory; it is taken from the PIC/S Guidance on Computerized Systems in GXP Environments (1).

[AUTHOR: Definition for OECD?] The OECD GLP Consensus Document on Computerized Systems document released in 1995 has the following to say on change control for computerized systems operating in good laboratory practice (GLP) environments under section 7c of the document (2):

Change control is the formal approval and documentation of any change to the computerized system during the operational life of the system. Change control is needed when a change may affect the computerized system's validation status. Change control procedures must be effective once the computerized system is operational.

The procedure should describe the method of evaluation to determine the extent of retesting necessary to maintain the validated state of the system. The change control procedure should identify the persons responsible for determining the necessity for change control and its approval.

Irrespective of the origin of the change (supplier or in-house developed system), appropriate information needs to be provided as part of the change control process. Change control procedures should ensure data integrity.

PIC/S Guidance for GXP Systems

18. Change Control And Error Report System (PIC/S Guidance 2003) (1)

18.1 The formal change control procedure should outline the necessary information and records for the following areas:

Records of details of proposed change(s) with reasoning.
System status and controls impact prior to implementing change(s).
Review and change authorisation methods.
Records of change reviews and sentencing (approval or rejection).
Method of indicating 'change' status of documentation.
Method(s) of assessing the full impact of change(s), including regression analysis and regression testing, as appropriate.
Interface of change control procedure with configuration management system.

18.2 The procedure should accommodate any changes that may come from enhancement of the system, i.e. a change to the user requirements specifications not identified at the start of the project. Or alternatively a change may be made in response to an error, deviation or problem identified during use of the system. The procedure should define the circumstances and the documentation requirements for emergency changes ("hot-fixes"). Each error and the authorised actions taken should be fully documented. The records should be either paper based or electronically filed.

18.3 Computer systems seldom remain static in their development and use. For documentation and computer system control it should be recognised that there are several areas that would initiate change or a review for change. These are:

A deviation report;
An error report; or
A request for enhancement of the computer system;
Hardware and software updates. •

Some of the key concepts from both documents about change control are:

- Formal process and formal approval.
- Scope covers both the computer system and the associated documentation (both written in-house and by a vendor).
- Formal evaluation of the change to understand its impact on the system and the users.
- Does the change affect your data?

Change Control and Configuration Management

Let's look at what is required for both change control and the associated process of configuration management.

There are a number of terms we need to consider here:

Change control: The systematic process by which any change to a computerized system is proposed, coordinated, evaluated, rejected, or approved and implemented (including testing and revalidation as necessary).

Configuration management: The system for identifying the configuration of hardware, software and firmware at discrete points in time with the purpose of systematically controlling changes to the configuration and maintaining the integrity and traceability of the configuration throughout the system lifecycle.

These two terms are very closely linked and some pharmaceutical organizations have condensed them to *change management* to cover all aspects of the control of a spectrometer (or any computerized system).

Note that configuration management also can be applied to software development and refers to the control of the versions of the software units and modules as the developers write them. For the purposes of the discussion here we will use it only in the specific context of the configuration of the operational computerized system and the spectrometer.

Two additional terms dealing with configuration management are:

Configuration item: Definition of the individual components in a configuration management system. Items can include hardware (spectrometer, server, and workstation), software (application, software utilities, operating system, service packs and patche, and peripherals (printers, plotters).

It is very important that each configuration item is carefully defined — if too detailed the change control and configuration management process will be too resource intensive and become an administrative nightmare to operate; if set too high the information generated will be useless.

Configuration baseline: The establishment of the initial configuration of the computerized system from the configuration items.

If a system undergoes rapid change or there are differences between the actual configuration and configuration log, it may be necessary to redefine the baseline (often called rebaselining). Furthermore, during an audit or an inspection, one will try to reconcile the configuration items in the log with the physical and logical ones on the instrument: the two should match exactly — many don't.

Change Control Process

A typical change control procedure is typified by the following criteria:

- Responsibilities of all parties involved are defined and known.
- Managed process.
- Documented process.

The overall process is outlined in Figure 1. The first part of the process is a request for change; this requires some basic information:

- Identify the person who requested the change.
- Description of the change.
- Justification for the change.
- Date of the change request.

The request for change may result from a variety of reasons. It may be the reporting of a bug or feature of the system software that should be resolved, the performance of the system is not adequate, or there is a request for additional resources such as a printer, workstation upgrade, or extra disk space.

Whatever the change requested, it needs to be documented. Documentation should be as simple as possible, keeping the paperwork to a minimum and encouraging all that use the system to comply with the process.

Second, the request needs to be analyzed for its impact. There are a number of factors to consider here: the effect of the change for its impact on the laboratory and the organization, and on the system itself. In looking at the impact of the change on the laboratory, one should consider

- Time required to implement the change.
- Cost of the change (including writing any documentation, any associated retraining caused by the change and also the time to test the change including any regression testing of the rest of the software to assess if the update has impacted another part of the application).
- Resources required (both physical and human) to make the change.
- Benefits of making the change.

When looking at the impact of the change on the system, consider

- Does the change provide a major or minor business benefit?
- Must the change be made for compliance reasons alone?
- Is the change for cosmetic reasons only?
- Is there any impact on the system?
- Are the functions already available or is an enhancement necessary?
- If the change is implemented will it cause any problems (regarding training, documentation, and so forth)?
- How much retesting and revalidation is required?
- What is the cumulative impact of incremental changes since the last full validation of the system?
- What is the effect of the change on the organization?
- Does the change bring a cost saving to the organization or is more cost required?
- Will the change allow for time or cost savings?
- What impact will the change have on the documentation of the system?
- What impact will the change have on the users of the system: will there be any necessity for retraining?
- What is the impact and cost of doing nothing?

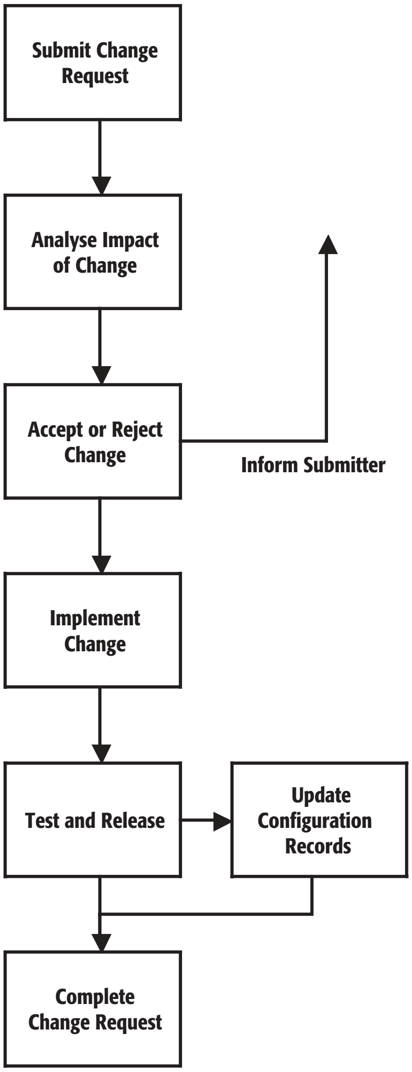

Figure 1: Change control process for a spectrometer system.

Once the impact analysis has been completed, the system owner can review each change with IT (if the system is networked) and QA. Alternatively, this can be devolved to a small validation or change control team consisting of two or so individuals authorized to consider and recommend changes. The size of the system, the business benefit and the magnitude of the change should decide the approach.

Here changes will be reviewed and can be classified into those that bring major or minor benefits. The prioritization of authorized changes will probably need to be balanced with the available budget and resources, as it is unlikely that all authorized changes will proceed. There will inevitably be change requests that are rejected for a variety of reasons. Regardless of the decision by the reviewing group, it is of supreme importance that decisions and the rationale for making them are fed back to the requester.

If the change is rejected the submitter will be informed of the rejection and the reason for it. However, if the request is approved, the resources are made available to implement the change. The first stage is to formulate a plan to implement the change; this will incorporate any relevant aspects of the impact assessment and any technical issues such as the extent of retesting and revalidation of the system update of documentation and retraining of users.

The change is then made and the system released for use. You should consider a test environment — for some systems a spare PC that you can use to evaluate the change and then complete the validation on the operational system. Before implementing the change be sure the operational system is completely backed up before you start, so that you have a fall back position in case anything goes wrong.

Typical System Changes

Figure 2 is a stylized view of a networked system with a workstation controlling a spectrometer where data are stored on a network server. Both the server and workstation consist of PC hardware, the operating system, and the spectrometer application software. Through this figure we can illustrate and discuss any changes to the overall system.

Consider the following possible changes to the system and the impact that each could have:

Changing the workstation: In this situation the whole application software needs to be reinstalled and therefore extensive revalidation of the system needs to occur. The spectrometer itself will not be impacted so the instrument will not have to be requalified; however, the control of the instrument by the new installation will need to be demonstrated.

Installing a service pack or patch for the spectrometer application: The release notes supplied by the vendor will outline the nature of the extent for change when the patch is installed. Typically you'll test the functionality of the patch works for your application. In addition, you can also undertake some regression testing of the main functions of the application such as if you re-interpret a data file will you get the same spectrum?

Installing a new version of the application software: When this happens it will typically be a complete revalidation of the system; check that AOD has not also installed a new firmware version at the same time.

The impact that each potential change could have on the validation status must be assessed. For example, the hardware change that included a processor upgrade is relatively small compared with the upgrade of a service pack for the operating system or a new version of the system software.

Not all changes can be planned; there may be time when your software fails due to a bug or virus. for example. Then the change control process needs to have a section dealing with how to handle emergency changes. Typically this will allow a few authorised people the ability to make the changes without filling in the change control form and get the system running again. Then the formal documentation is completed and approved retrospectively.

Defining the Detail of Configuration Items

How far do we need to go when we define the detail associated with configuration items? Let's look at what we could do for a portable PC; here are some options:

- Toshiba Tecra M1
- Toshiba Tecra M1,
- 1.6-MHz Centrino processor,
- 512 MB RAM,
- 80-GB hard drive,
- CD-ROM RW
- Operating System Windows XP Pro, Service Pack 1
- Serial Number 553217886 TBY

- Toshiba Tecra M1
- 1.6MHz Centrino processor,
- 512 MB RAM,
- Teac DZ 990T 80-GB hard drive,
- Teac DW 224E CD-ROM RW
- Operating System Windows XP Pro, Service Pack
- Serial Number 553217886 TBY
- BIOS version 1.20
- Display 1068 x 764 resolution

Option one is very simplistic and you can't go into much detail. If anything is changed (memory increased) you can't tell because there is no baseline configuration information to compare with. The PC could be swapped with an equivalent model and you wouldn't know.

Option two gives more information that is relatively easy to collect and maintain. The PC is uniquely identified via its serial number so that you know the system is the right one. The information here, however, does not tell you about any security patches that have been applied to the operating system.

Option 3 is more detailed compared with the other two; however, you'd have to spend more time collecting and maintaining the configuration, which may be unrealistic. Configuration management information therefore is based around option 2 for defining the configuration item as a general rule.

There may be exceptions where specific boards or hardware are added to control the spectrometer. These of course would need to be added to the configuration item list.

Defining the Baseline Configuration of the System

This is the process of compiling the list that consists of all the configuration items components of the system including:

- All the release numbers and serial numbers (where appropriate) of the application software programs.
- The software tools (for example, database) and the operating system.
- The components comprising the hardware should be used such as disks, memory, type of central processing unit, add-in boards for the application or communications.
- Spectrometer.

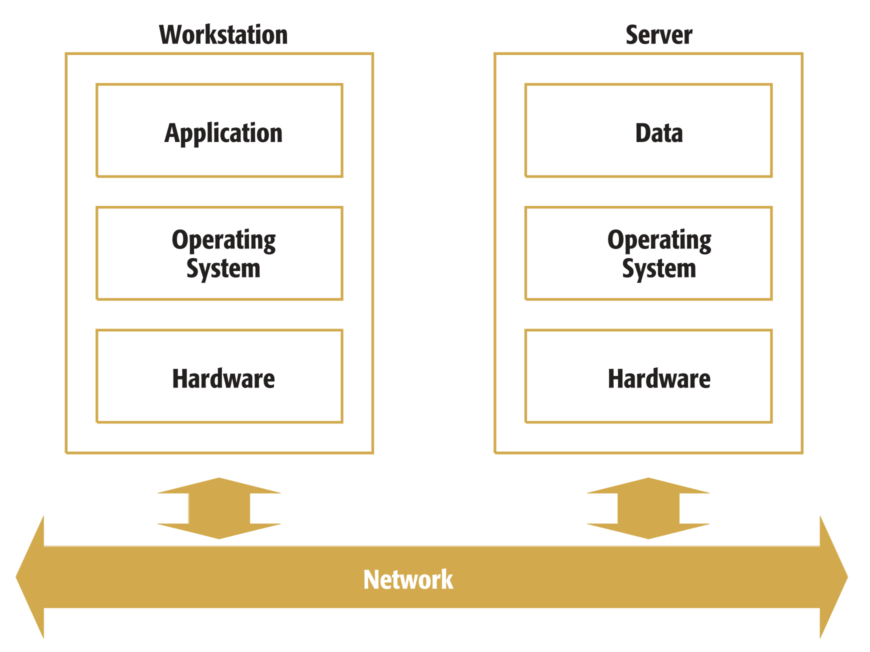

Figure 2: Outline configuration of a spectrometer workstation to a networked data server.

- Any peripherals.
- System documentation should also be included in the configuration management log.

The baseline configuration should be established at the installation of a new system. This has a number of advantages: first, all testing and training takes place in a controlled environment, and second, the procedures and principles of configuration management are known and understood, and modified if necessary, before the system is rolled out for operational use. The information for the baseline configuration will come from the purchase order, and this will be checked off at the installation.

Linking Configuration Management with Change Control

When a change control request is approved and implemented, the change may replace or change a configuration item. Then the new configuration and the date from which it is effective is noted in the log. When new versions of the software are available and installed, master copies of the old version and the relevant documentation should be archived, as they should be considered equivalent to raw data.

Summary

Procedures for change control and configuration management need to be established to ensure that the validation status of any system is maintained throughout the lifetime of its operation. These procedures provide the mechanism for ensuring that changes are made in a defined and controlled manner (with the exception of emergency changes that the system managers can make under pre-defined situations) and through the current and historical records, an exact configuration of the system on any day can be reconstructed. From the scientific and regulatory perspectives, this provides the information to assess the impact of an item of the system and how long it was operational. They provide records to demonstrate how stable the system was (or not).

References

Good Practices for Computerised Systems in Regulated GXP Environments, Pharmaceutical Inspection Co-operation Scheme (PIC/S), Geneva, Switzerland, 2003 (www.picscheme.org).

Application of the Principles of GLP to Computerised Systems, Environment Monograph 116, Organisation for Economic Co-operation and Development, Paris, France, 1995.