System Configuration Management and Version Control in an FDA Regulated Environment

Author Name     Steve Zarichniak
Title       Applications Consultant
Company      Honeywell
Address       1100 Virginia Drive
City/State/Country/Postal Code  Fort Washington, PA 19034
Telephone/Fax     215-641-3244
E-mail      steve.zarichniak@honeywell.com

KEY WORDS
Version control, Lifecycle management, Qualification process, Genealogy, Phase control, 21 CFR Part 11

ABSTRACT
Managing the genealogy of database configuration and its life cycle is critical to following 21 CFR Part 11. In addition to recipes and equipment model configurations, phase logic and control strategies residing in automated control systems are an integral part of automated batch execution. Typical configuration management systems do not provide the capability to implement and guarantee a standard development procedure for the database configuration. With a set of enforced qualification states and GAMP-based transitions, a strategy that has been properly tested and approved with signatures can be installed on a process system. For control systems operating in validated environments, this procedure is paramount. This paper explores the life cycle management requirements for batch phase logic and control strategies executing in a validated environment.
System Configuration Management and Version Control in an FDA Regulated Environment

Introduction
For manufacturers subject to regulations enforced by the FDA in the United States and other agencies worldwide, it is critical that processes and systems are validated.

This document provides a description of the validation process and discusses how configuration and lifecycle management can assist users with system validation.

By definition, a product or device cannot be compliant because the validation criterion depends on the customer’s processes and how they will operate and maintain their systems.

Validation
"Establishing documented evidence which provides a high degree of assurance that a specific process will consistently produce a product meeting its pre-determined specifications and quality attributes."¹

The purpose of validating automation systems is to prove with a high degree of assurance that the system will work correctly and consistently. For 21 CFR Part 11 compliance, validation should also prove the accuracy and reliability of the data collection and management system. Developing documented evidence typically progresses logically through the following five steps:

1. Planning – Preparing a written validation plan.
2. Specifications – Specifying and agreeing to what is required.
3. Test Planning – Preparing Installation Qualification, Operational Qualification & Process Qualification documents to describe how the equipment/system is to be tested.
4. Testing – Performing the planned tests according to the documents and collecting the results.
5. Review – Reviewing the results to show that the system performs as specified


Copyright © 2003 World Batch Forum. All rights reserved.
System Life Cycle
Effective validation needs to be an integral part of the system life cycle. The system life cycle describes the major activities involved in implementing, maintaining, using and eventually retiring systems. Figure 2 illustrates a life-cycle development framework covering specification, design, construction, testing, installation, acceptance testing, operation and retirement. “Specification” through “Acceptance Testing” describes the subset for project activities related to the initial installation and future improvement activities to a system, i.e. Management of Change.

Figure 2: System Life Cycle
Project Framework
Project framework is a subset of the total system life cycle. Figure 3 shows the life cycle phases that are part of any project framework and how they relate to one another.

Validation is an integral part of project implementation in FDA regulated industries. As such, validation needs to be integrated into the project life cycle. Figure 3 illustrates when validation documents and test protocols need to be developed and the order of execution of the test protocols. The Performance Qualification Test Plan, Operational Qualification Test Plan, and the Installation Qualification Test Plan are commonly referred to as the test or validation protocols.

Below is an overview of the lifecycle phases and the activities performed in each phase.

Figure 3: Basic Framework for Project Specification, Design, and Testing
System Configuration Management

Management of change is a critical element in achieving and maintaining validation. Version control manages access to control strategies, but it does not provide an ability to define and manage the life cycle of control strategies. Life cycle management is used:

- To define the qualification states control strategies will go through from inception to decommissioning,
- For the approvals required to move from one qualification state to another, and
- To control what qualification state a strategy must be in to be downloaded into a controller.

The user must define life cycle management. Users define the life cycle by configuring the qualification states, the transitions between the states, the transition permissions and electronic signature behavior.

Table 1 illustrates state and transition definitions. The “From State” column on the left lists the user-defined qualification states that make up the life cycle. To define the transitions, the actual states are listed horizontally under the “to State” heading. The user defines both the permissible target states for each state and the necessary approval signatures. Using the “Implemented” actual state as an example, to move a strategy from “Implemented” to “Ready For Test”, a member of ENGR security group must approve the action. Also, in this lifecycle, a member of ENGR can approve changing the qualification state of a strategy from “Implemented” to “Non Regulated.” This lifecycle configuration prohibits changing a strategy in the “Implemented” state to the “Ready for Verification” state.

Table 1: Example of Qualification States and Transitions
Table 2 shows the signature definition. Again using the “Implemented” actual state as an example, a user must supply their User ID and password to move a strategy from “Implemented” to “Ready for Test,” but no signature is required to move from “Implemented” to “Non Regulated.”

![Image of State Transition Requirements](image)

Table 2: Example of Signature Requirements

Once configured, the system configuration lifecycle as defined by the user is enforced. It provides an audit trail of all changes, records electronic signatures where required and provides tools to view differences between versions. In addition, the user establishes rules regarding which qualification states the strategy must be in to be downloaded.

System Configuration Management should provide not only version control but configuration life cycle management and control of strategy downloads. This ensures system strategies are managed consistent with the user’s development and validation process requirements.

To be consistent with 21 CFR Part 11, system configuration and life cycle management applications require robust levels of system security, information management and controlled system access. These aspects are discussed below.

**Information Management and Audit Trails**

There are several aspects to information management. Data must be stored so it cannot be adulterated, the user maintains the ability to access and retrieve data throughout its retention period and electronic signatures associated with the data cannot be modified or removed. This information is stored in formats that are not designed to permit editing or modification of the files or the data within the files.
All operator actions are recorded and stored in the event file. Information stored includes timestamp and the full printed name. The electronic signature (operator ID) is associated with an electronic record at the time of entry and cannot be separated. This results in a complete audit trail of all actions performed on the system. Administrative actions such as changes to operator definitions, operator area assignments and definition of sign-on restrictions are also recorded to the event file so that the audit trail also contains a history of administrative actions. The full printed name or operator ID can be displayed when the event files are viewed or printed or when the data is included in a report.

**System Access and Security**
System security, control access, security levels, control levels and area assignments for each individual operator or alternatively for each operator station must be maintained.

Operator sign-on/sign-off security provides control levels to limit operator control of individual items of plant and equipment. Security levels define a user’s function: operator, supervisor, etc. The system should be able to be partitioned into areas to control access to a particular section of the plant or process.

Any actions initiated by an operator must be logged in a journal complete with the full printed name as part of the record. In addition, any control action to a given point is only allowed if the control level configured in the operator profile exceeds the level assigned to the point.

**Conclusion**
Version control for system configuration is an important feature used to meet validation requirements, but it does not manage system configuration life cycle. Adding life cycle management features to an automated version control system allows users complete management of their system configurations with these benefits:

- Cost savings for IQ, OQ and PQ development
- Lower risk – less paper work
- Lower up front project management
- Lower lifecycle costs
- Improved compliance

**Terminology**
- **Qualification life cycle** - capability to enforce GAMP guidelines regarding control system development.
- **Objects definition** - all tagged objects in the automation system
- **Version repository** - the repository with all versions of each configured object
- **Check-out** - means locking a particular version of an object in the management system and allow it to be changed by a single user.
- **Check-in** - place a new or modified object under version control.
• **Audit trail** - a log of all interactions for auditing purposes.
• **Revert** - the retrieval of a specific version of an object or set of objects.
• **Revert label** - a means to identify a set of unique objects.

**Definitions**

• **Electronic Record**: any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

• **Electronic Signature**: means a computer data compilation of any symbol or series of symbols executed, adopted or authorized by an individual to be the legally binding equivalent of that individual's handwritten signature.

• **Digital Signature**: an electronic signature based on cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

**References**

• 21 CFR Part 11
• 21 CFR Part 210, 211
• GAMP Guide to Validation of Automated Systems in Pharmaceutical Manufacturing, April, 1998