DeltaV Capabilities for Electronic Records Management

An integrated solution for meeting FDA 21CFR Part 11 requirements in process automation applications using a configurable off-the-shelf (COTS) solution

Contents

FIGURES

TABLES

Introduction

The United States Food and Drug Administration (FDA) has a legal responsibility to ensure that drugs are safe and effective. Therefore, in FDA-regulated industries, quality and accountability standards are much higher. One of the ways the FDA assures quality in the industry is to require that records concerning important aspects of the manufacturing process be kept. FDA regulations concerning manufacturing and related record keeping are known as the Current Good Manufacturing Practices or cGMPs. These regulations orginally dealt with paper records and hand-written signatures. However, with the rise of computer technology used in food and drug manufacturing, it became apparent that regulations were needed to address the issues related to electronic records and signatures. A joint FDA/industry task force was formed to develop the requirements for electronic records and signatures, resulting in the 21 CFR Part 11 regulation that became law in August of 1997.

The objective of 21CFR Part 11 is to allow the industry to take advantage of electronic record keeping while making sure that electronic records and signatures are equivalent to paper records and signatures. The regulation defines what the FDA requires to ensure that electronic records are reliable, trustworthy, and authentic and that they can be considered equivalent to paper records and handwritten signatures for FDA purposes. This rule does not mandate the use of electronic records; however, if electronic records are used to keep FDA-required information, then the electronic records must comply with 21 CFR Part 11.

The fundamental activities related to process automation where cGMP records are created are in the areas of project engineering, manufacturing operations, system administration, and system maintenance. All through these activities, records needed to meet FDA requirements are generated. To the extent that any of these documents are stored electronically, they must comply with the 21 CFR Part 11 rule.

This whitepaper examines cGMP records that are potentially within the domain of process automation and illustrates how the DeltaV system provides off-the-shelf technology to support a Part 11-compliant solution for cGMP records. The body of this whitepaper provides an overview of the DeltaV system and how it supports Part 11 compliance. A more detailed “rule-by-rule” analysis is presented in tabular form in Appendix A.

Procedural and Technical Controls

Controls required for 21 CFR Part 11 compliance can be classified into two categories: procedural and technical. Procedural controls are practices that affect how the system is used. They are not part of the hardware and software of the system. An example of procedural control is a procedure for providing access to only authorized individuals. The end user must provide the procedural controls.

Technical controls are characteristics of the system itself. An example of technical control is a user management scheme that allows different users different levels of access. The process control system vendor may provide the technical controls as the standard functionality in a commercial off-the-shelf (COTS) product. Alternatively, technical controls may be part of a custom application.

In some cases, custom applications or third-party add-ons may be used on top of the automation system to address weaknesses. However, in general, using COTS products, minimizing the integration of multiple applications, and avoiding custom applications make the system more maintainable. As a result, selecting a process automation vendor should involve selecting the supplier who can meet the most of your requirements with standard features.

Integrated Features and Custom Applications

The DeltaV system is a commercial off-the-shelf (COTS) product that supports Part 11 compliance with features such as:

- Version Control and Audit Trail (VCAT)
- Recipe Authorization
- Operator Actions with Confirm/Verify
- Batch Historian
- Operator Electronic Log

Because these integrated features are built into the DeltaV system as standard product, upgrade and maintenance issues that would fall upon a non-integrated system are greatly reduced. A non-integrated control system with custom applications from different vendors would face many procedural controls and validation issues that can be best avoided with an integrated system like the DeltaV system. These features and others will be discussed in this document with reference to the applicable 21 CFR Part 11 section.

Aspects of 21 CFR Part 11

Subpart B—Electronic Records

Section 11.10 Controls for Closed Systems

21 CFR Part 11 defines the requirements for considering electronic records and electronic signatures to be equivalent to paper records and handwritten signatures on paper. The rule is applicable to records in electronic form that are created, modified, maintained or transmitted to the FDA .

In the following paragraphs, specific sections of 21 CFR Part 11 are discussed with reference to how DeltaV (v7.3) software supports Part 11 requirements. DeltaV support of compliance is discussed (where applicable) with reference to the application program that manages or generates the electronic record. For example, discussions will include configuration engineering, run time, and history applications.

11.10(a) Altered Records

One of the requirements of Section 10(a) is the ability to discern an altered record. One of the best ways to prevent a record from being altered is by restricting access to the system or record. DeltaV Flexlock provides a mechanism that restricts DeltaV users from having access to the Microsoft Windows desktop or configuration applications.

For users who need access to perform configuration changes, the DeltaV Configuration Audit Trail, when enabled, documents all changes to the system configuration. The ability to disable the audit trail feature is controlled by DeltaV security.

History applications do not allow access to data files by anyone who does not have System Administrator privilege. The historical data files are write-protected with write-access being given only to the applications that need to write data to those files. As such, it is not possible for a user who does not have system administrator privileges to make

modifications to a file. In addition, system security may be set up to prevent accessing data at the file level by preventing access to the Windows desktop and with the use of Windows file security that can enable data files to be read-only.

The DeltaV system is built upon standard Windows-based software and data management tools that will allow data to be accessed and potentially modified by an administrator. The industry recognizes this as an issue and, based on current technologies, must use procedural approaches to safeguard data. The general approach is to give administrative privilege only to personnel not responsible for manufacturing production. Therefore, the system administrator would have no incentive to falsify data. Data falsification would occur only if there were collusion between an administrator and another person who had a motive to falsify the data.

11.10(b) Reproduction of Records

Section 11.10(b) requires that the electronic records can be copied in *"human readable and electronic form suitable for inspection, review, and copying by the Agency".* The DeltaV system allows configuration data to be printed from the configuration applications. Configuration audit trail information may also be viewed online and printed. History applications allow electronic viewing and printing of data.

Electronic copying of DeltaV electronic records may be done in the native DeltaV file and database formats, or can be exported in different file formats including text, Microsoft Word, Microsoft Excel, and MS Access, using tools included with the DeltaV system.

11.10(c) Protection of Records

Section 11.10(c) requires the *"protection of records to enable their accurate and ready retrieval throughout the records retention period".* As discussed earlier in Section 11.10(a), protecting files and limiting access to DeltaV features is one of the best ways to protect records. The DeltaV system has built-in security that controls access to DeltaV configuration applications and database administration tools. One of these tools is DeltaV Flexlock, which provides a mechanism to prevent DeltaV users' having access to the NT desktop or a DeltaV database account.

The history applications provide data archival support to allow for their accurate storage and retrieval. The Batch Historian Administrator application does not allow for the deletion of a batch history that has not been archived. The Batch Historian Administrator is an application that allows personnel with the required security access to archive and catalog batch records, operator action records, and alarm records to a permanent storage location. Archiving may be done manually or on a scheduled basis. The Batch Historian Administrator documents all archiving events by providing an audit detail view.

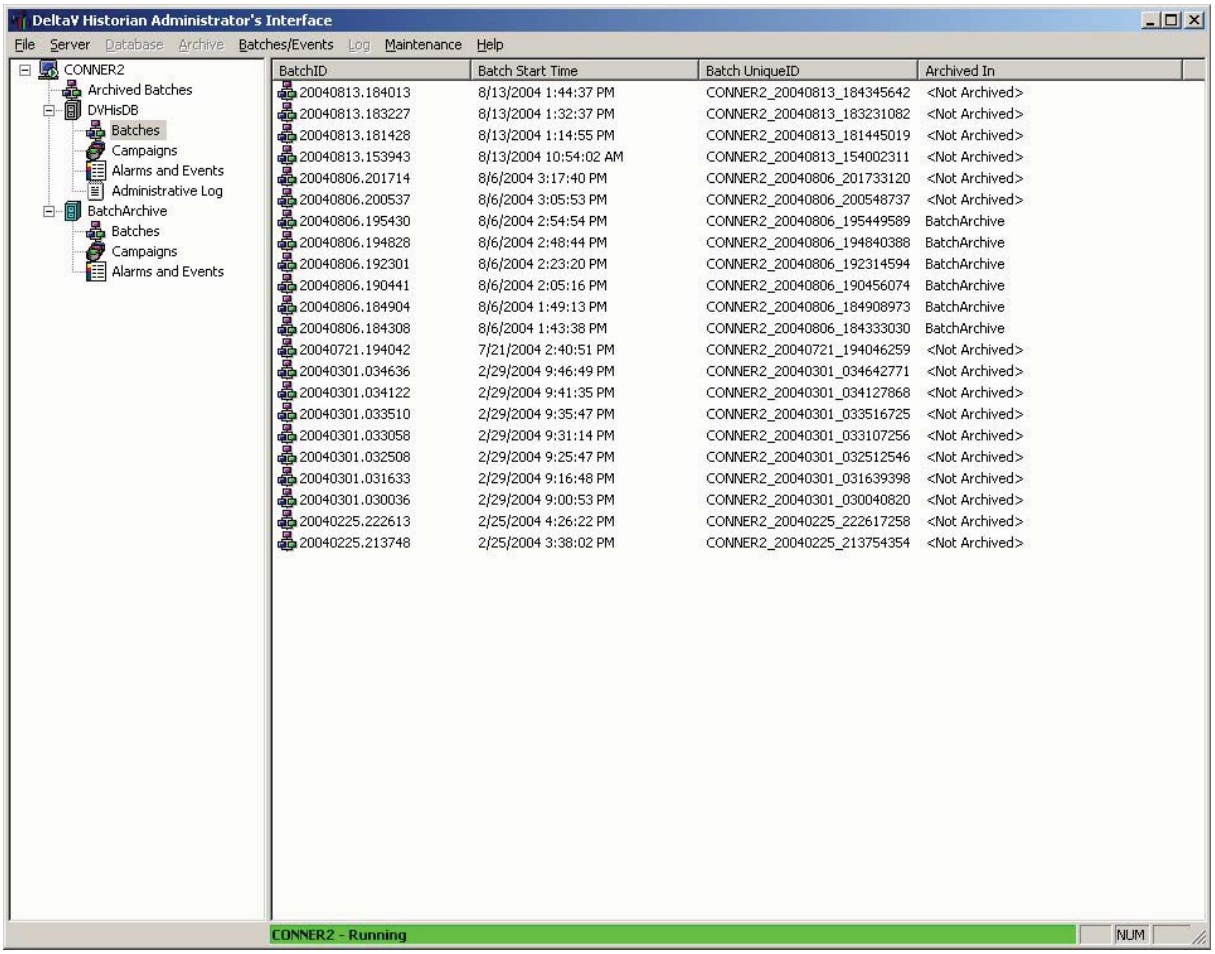

Figure 1 Batch Historian Administrator supports archiving of electronic records manually or on a scheduled basis.

11.10(d) Limiting Access to Authorized Individuals

Limiting computer system access to authorized individuals promotes data authenticity and integrity. The DeltaV system has built-in security that controls access to DeltaV configuration applications and database administration tools. It has a sophisticated security system that is layered on the Windows security system. Access can be limited to specific users on a function and area basis. A user may be granted system access for only the specific functions that his or her responsibilities and training dictate. This provides the ability to grant system access by area, by system function, and by parameter.

The DeltaV security system is designed around the concept of “locks” and “keys”. System functions, fields, and parameters are assigned to system locks. Users can access the function, field, or parameter only if the user's account is assigned the key to the lock for the function, field, or parameter.

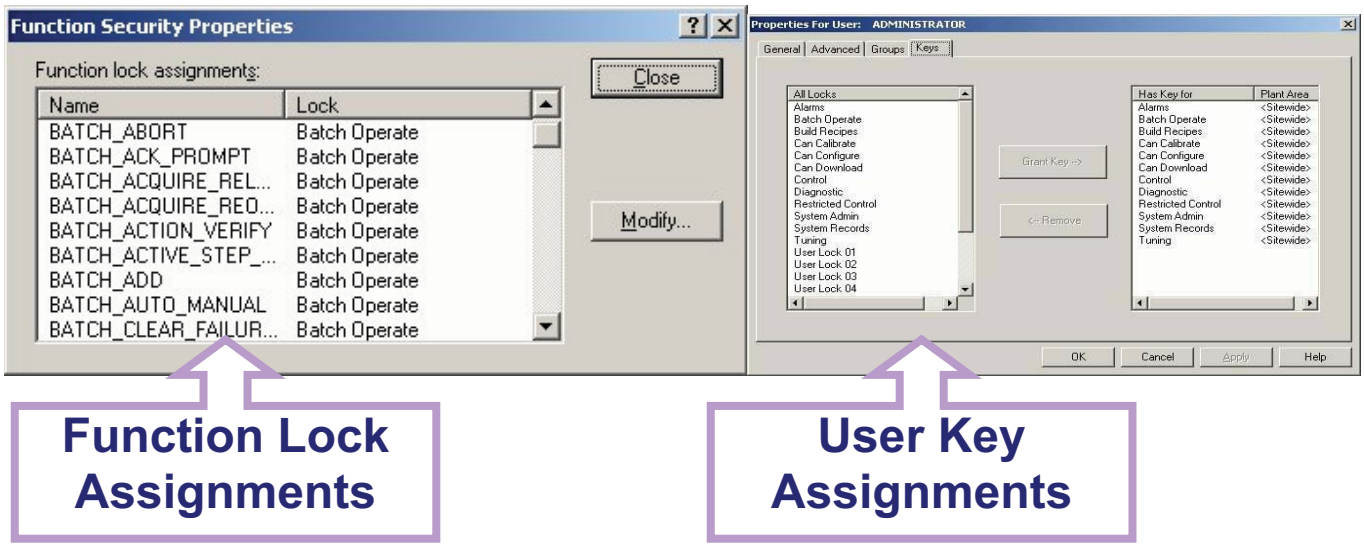

Figure 2 Single security system for all DeltaV applications controls the level of system access for each user.

In addition, DeltaV Flexlock can control access to the Windows operating system, Desktop, the DeltaV application and other applications based on user groups as defined by the system administrator. For example, a particular user group could be granted access to the DeltaV system and denied access to the Windows operating system and the Desktop. Or the user group could be granted access to each of these applications.

11.10(e) Audit Trails

Section 11.10(e) requires the *"…use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records".*

Configuration Application

Engineering revisions and changes can be tracked as changes are made using the DeltaV Configuration Audit Trail and Version Management application. This application creates and maintains a configuration change history for configuration items. Information captured by the audit trail includes who made the change, the date and time the change was made, the exact scope of the change, and any comments entered by the engineer making the change. Version to version "differences" can be viewed online and printed. A rollback feature allows restoring to previous versions of a configuration item.

The following table offers a summary of DeltaV electronic data for which audit trails are provided.

Table 1. DeltaV Audit Trail Capabilities

Item	Audit Trail Implementation
Operations	
Operator Actions	DeltaV Event Journal
Alarms	DeltaV Event Journal
Interlock Trip	DeltaV Event Journal
System Events	DeltaV Event Journal
Batch Processing	
Phase State Changes	Batch Historian
Failure Conditions	Batch Historian
Start/Stop Procedure	Batch Historian
Start/Stop Unit Procedure	Batch Historian
Start/Stop Operation	Batch Historian
Start/Stop Phase	Batch Historian
Operator prompts	Batch Historian
Operator prompt response	Batch Historian
Formula Parameters	Batch Historian
Report Parameters	Batch Historian
Ad Hoc Operator Comments	Batch Historian
Acquire Unit	Batch Historian
Release Unit	Batch Historian
System Configuration	
DeltaV Control Configuration	
Control Modules	DeltaV Version Control and Audit Trail
Equipment and Control Module Classes	DeltaV Version Control and Audit Trail
Phase Classes	DeltaV Version Control and Audit Trail
Phase Modules	DeltaV Version Control and Audit Trail
Operations	DeltaV Version Control and Audit Trail
Unit Procedures	DeltaV Version Control and Audit Trail

Item	Audit Trail Implementation
Procedures	DeltaV Version Control and Audit Trail
Unit Classes	DeltaV Version Control and Audit Trail
Unit Modules	DeltaV Version Control and Audit Trail
Process Cells	DeltaV Version Control and Audit Trail
Process Areas	DeltaV Version Control and Audit Trail
Report Parameters	DeltaV Version Control and Audit Trail
Unit Parameters	DeltaV Version Control and Audit Trail
DeltaV Alarm Configuration	
Alarm Types	DeltaV Version Control and Audit Trail
Alarm Limits	DeltaV Version Control and Audit Trail
Alarm Priorities	DeltaV Version Control and Audit Trail
Alarm Display	DeltaV Version Control and Audit Trail
Security	
Parameter Security	DeltaV Version Control and Audit Trail
Field Security	DeltaV Version Control and Audit Trail
Function Security	DeltaV Version Control and Audit Trail
System Hardware Configuration	
Control Network	DeltaV Version Control and Audit Trail
Controllers	DeltaV Version Control and Audit Trail
Operator Stations	DeltaV Version Control and Audit Trail
DeltaV workstations	DeltaV Version Control and Audit Trail
System Admin Activities	
Security	
Define Valid Users	Windows Security Log
History Archiving	Batch Historian Administrator Tool

Run Time Application

All operator actions are recorded in a secure time- and date-stamped electronic record. Within the DeltaV system, electronic records are not able to be modified or deleted.

Batch History Application

Batch-related events are captured as an electronic record in the Batch Historian and include time and date stamp, the identity of the person making the change, and the location from which the change was made. The DeltaV system provides no access to modify records. These events may be deleted from the system only after they have been

archived. An audit trail is maintained in the Batch Historian Administrator that documents any time events are deleted after they have been archived by users with the proper access privilege.

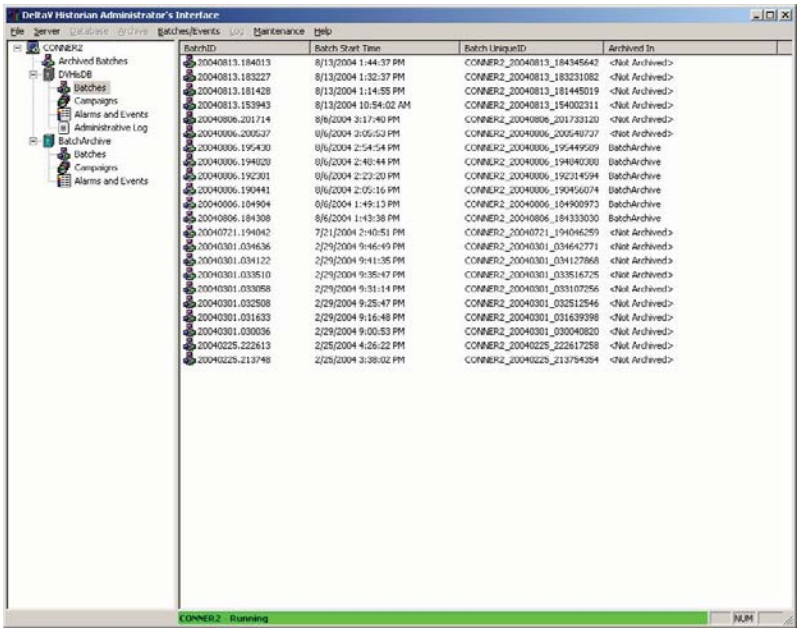

Figure 3 The Batch Historian captures batch records in a secure SQL server database with no configuration required.

11.10(f) Enforce Permitted Sequencing of Steps and Events

Section 10(f) states that procedures and controls shall include *"…operational system checks to enforce permitted sequencing of steps and events…."* In batch processes, sequences of events are predefined (pre-configured) by the recipe and must be followed when executing a batch. If changes are made to the batch sequences, those changes should be tracked and allowed only by personnel with the appropriate authorization.

Authorized personnel can configure the DeltaV Batch Operator Interface and Campaign Manager applications to require **Confirm** and **Verify** authentication. Using this feature, any change in batch operation will require **Confirm/Verify** before a change can be made. (See Figure 4 below.) Additionally, the DeltaV system restricts operator access by requiring an operator to have the security key(s) for the area the action is being taken in.

11.10(g) Use of Authority Checks

Section 11.10(g) requires the *"…use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand."*

Configuration Application

The DeltaV system is protected by a security system integrated into a standard Windows security that allows only authorized users with the correct level of access to perform tasks within the system. DeltaV has built-in security that controls access to DeltaV configuration applications and database administration tools. One of these tools is DeltaV

Flexlock, which provides a mechanism to prevent DeltaV users' having access to the Windows desktop or a DeltaV database account.

Run Time Application

Operator actions from Batch Operator Interface and Campaign Manager can be configured to require confirmer and verifier authentication. Operator prompts can be configured to require confirmer and verifier authentication. The confirmer and verifier must have the correct security key(s) for the area in which the action is being taken.

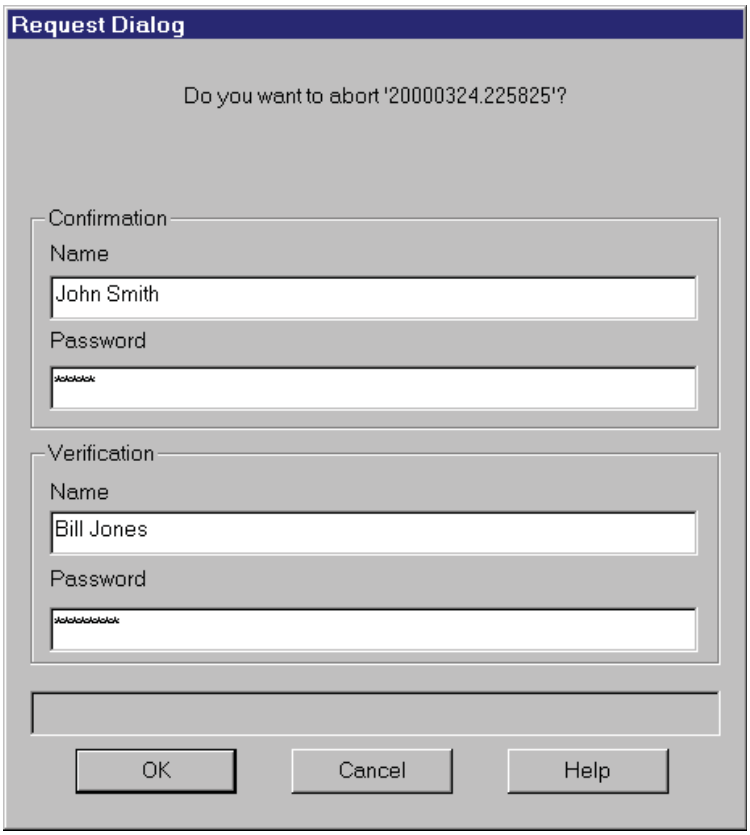

Figure 4 Operator Action Confirm and Verify

Batch History Application

Batch-related events are captured as an electronic record in the Batch Historian and include time and date stamp, the identity of the person making the change, and the location from which the change was made. DeltaV provides no access to modify records. These events may be deleted from the system only after they have been archived. An audit trail is maintained in the Batch Historian Administrator that documents any time events are deleted after they have been archived by users with the proper access privilege.

11.10(h) Device Checks

Section 11.10(h) concerns the *"…Use of device (e.g. terminals) checks to determine, as appropriate, the validity of the source of data input or operational instruction."*

The validity of the source of DeltaV data input is restricted to DeltaV terminals for entering data and taking control actions. The DeltaV system enforces validity checks by requiring that a device must be downloaded from the DeltaV engineering stations to become a valid device.

System users with proper security privilege can establish communications with input and output devices that are outside the DeltaV system. However, any interface between the DeltaV system and devices outside the DeltaV system is the responsibility of the customer.

11.10(i) Education, Training, and Experience for System Administrators

Section 11.10(i) requires that the persons who administer electronic signature systems have the education, training and experience to perform their assigned tasks. It is the customer's responsibility to ensure that all persons involved with a regulated system have the necessary levels of education, training, and experience to perform their assigned tasks.

11.10(k) Control over System Documentation

Part 11 section 11.10 (k) requires *"…adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance".* DeltaV security restricts access to system configuration documentation to those who are given access rights to the system configuration. This section also requires "*revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation."* The DeltaV configuration version control and audit trail capability is a complete change management system that ensures all configuration changes are done under strict revision control with an audit trail to document all system changes. Control configuration (control modules, unit modules, procedures, unit procedures, operations, etc.) must be first checked out to an authorized user before any changes can be made.

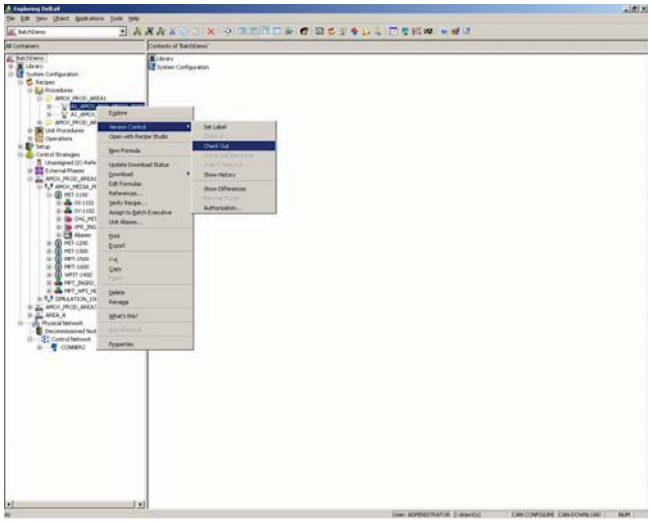

Figure 5 DeltaV Explorer provides visual indication that a Module is checked out for changes.

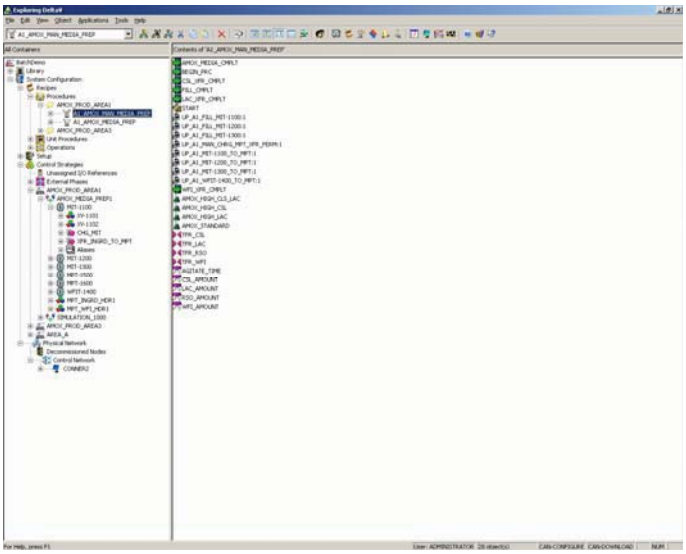

Figure 6 Module checkout for Version Control and Audit Trail

When a module is checked out, it may be modified and changed over a period of time by a user. Not until the module is checked in does it formally become part of the updated system configuration, as this prevents accidentally downloading configuration for any modules that are a work in progress. Upon check-in, the user is allowed to enter a comment describing revision history, and the module version number is automatically updated when check-in is completed.

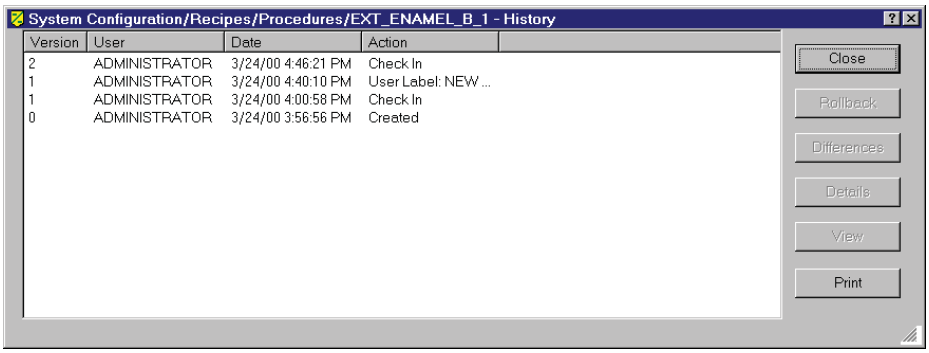

Figure 7 Version Control and Audit Trail automatically creates versions as changes are made and keeps complete history of all versions.

The DeltaV Version Control and Audit Trail feature keeps a complete history of all engineering revisions. The history feature allows viewing of all versions of any module and a difference report may be generated between any two versions of a module. The difference report can be viewed either graphically or textually with differences color-coded to indicate items that have been added, deleted, or changed.

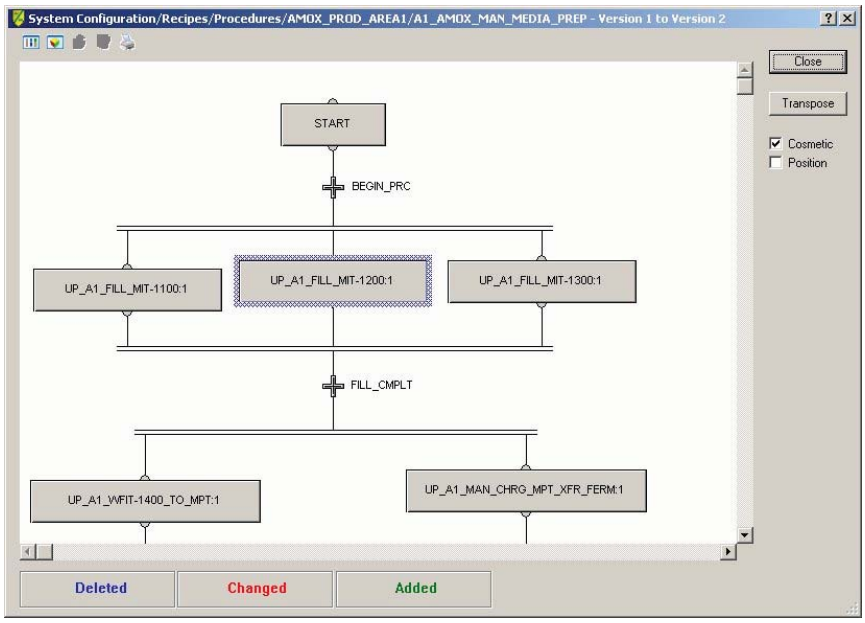

Figure 8 Difference reports may be generated between any two versions. Graphical difference report indicates what has been deleted, added, or changed.

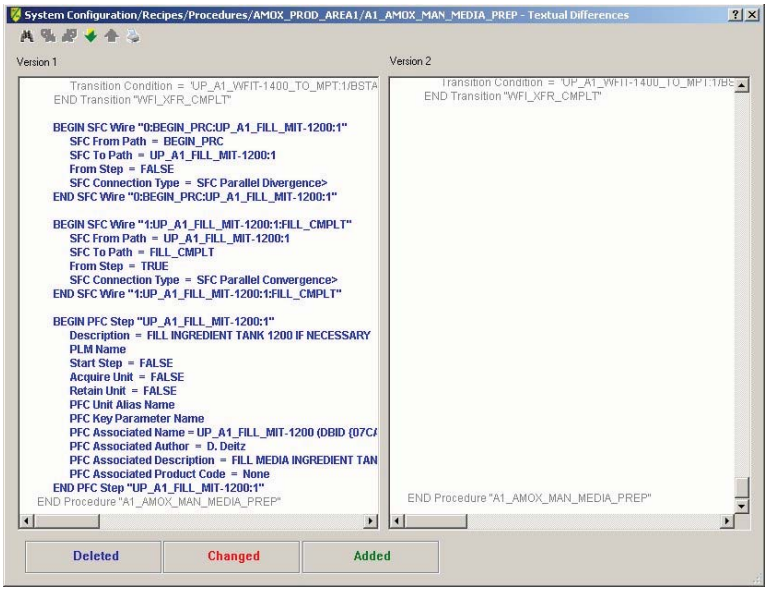

Figure 9 Change report shown in text view

The rollback feature provides the ability to select any previous version and make it the current version. When a rollback is performed, a new version that is identical to the selected version is created, preserving all the history of

the module. The module history includes download events, which details the module versions that have been downloaded to the running controller.

Some systems depend upon external code management systems such as Microsoft Visual SourceSafe to implement code management. External systems are disconnected and do not provide the full benefits of an integrated source code management system. For example, they cannot capture download events and document which versions are actually running in the controllers; nor can they give warnings during downloads that a module is currently checked out for modification.

Recipe Authorization

The recipe authorization feature may allow from one to five user approvals before a recipe can be released to production for use. The recipe authorization is tightly integrated with the Configuration Audit Trail and Version Management to track recipe changes, approvals, and comments. Unapproved recipes cannot be downloaded.

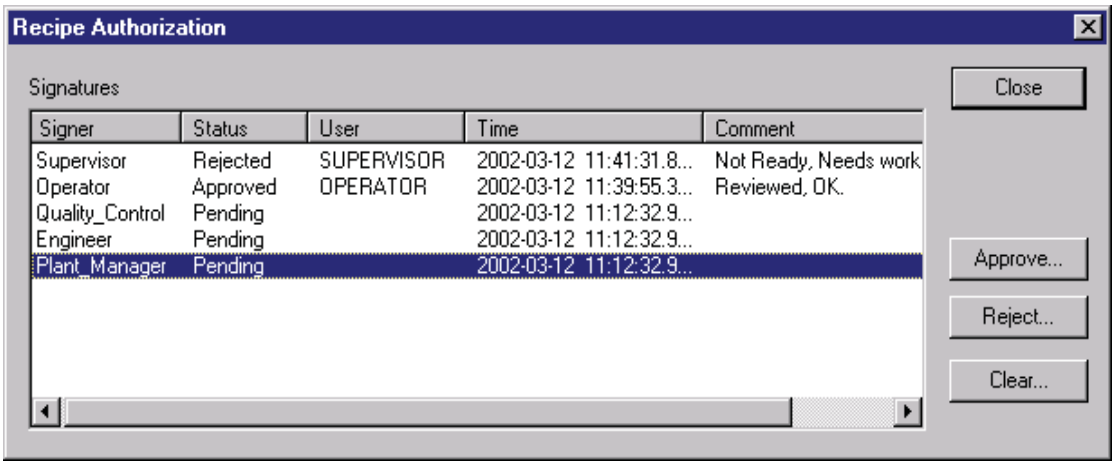

Figure 10 Recipe authorization may require from one to five user approvals before a recipe can be downloaded.

11.30 Controls for open systems

Section 11.30 requires that persons who use open systems to create, modify, maintain, or transmit electronic records shall employ additional controls such as document encryption and digital signatures to ensure the records' authenticity and integrity. By definition, an open system is an environment in which system access is not controlled by persons responsible for the content of electronic records on the system. In a DeltaV system, the system administrator controls system access to the electronic records in the system, making it a closed system. Therefore, the Section 11.30 requirement for open systems does not apply to a closed system such as the DeltaV system.

11.50 Signature Manifestations

The FDA requires that signed electronic records clearly indicate the printed name of the signer; the date and time of the signing; and the meaning of the signing. Signed electronic records must be subject to the same controls as electronic records and linked to their respective electronic records.

The DeltaV system is configurable to generate messages prompting signature inputs that allow for: the user name of the signed; the date and time of the sign, which is recorded in historical data records; and the meaning of the signing **(Confirm/Verify** of operator actions or prompts).

11.70 Signature/Record Linking

Section 11.70 requires that electronic signatures and handwritten signatures executed to electronic records be linked to their respective electronic records, so that the signatures cannot be excised, copied, transferred, or falsified.

In the DeltaV system, the electronic signatures are an integral part of the batch history and are linked to their respective batch records. DeltaV data view and analysis tools do not provide any mechanism to allow the modification or deletion of a record.

Subpart C—Electronic Signatures

11.200 Electronic Signature Components and Controls

Section 11.200 requires, for non-biometric electronic signatures, two identification components: an identification code and password. This requirement also applies for signings not performed during a single continuous period.

The DeltaV **Confirm and Verify** signature feature requires specific sign off with user name and password on any action configured to require a signature regardless of who is logged onto the system. The DeltaV system also offers the added convenience to allow others not logged on to sign off on actions that they have authority to take. The **Confirm and Verify** features are available with DeltaV Operate, the Batch Operator Interface and Campaign Manager applications.

Section 11.200 requires that signatures be used only by their genuine owners and that attempted use by an individual other than the genuine owner require collaboration of two or more individuals. The user name and password components for DeltaV electronic signatures are extensions to the Windows security system. Windows passwords are encrypted and not accessible even by the system administrator. Any use of a signature by someone other than the genuine owner would require the collusion of the genuine owner.

11.300 Controls for Identification Codes and Passwords

Section 11.300 defines requirements for using and maintaining user identification codes and passwords. This section requires that user identification codes (user id) and password combinations be unique for each person, that they be periodically changed, that loss management procedures be in place in the event that the user I.D. and passwords are lost or compromised, and that safeguards be in place to detect and prevent unauthorized use of user I.D.s and passwords.

Since DeltaV user I.D.s and passwords are part of the Windows security system, they have available the full functionality of the Windows security system that enforces unique user I.D.s and passwords and that allows the administrator to specify password lengths and expiration policy. Windows security allows the administrator to set the lockout policy such that failed login attempts can lock out a user and require the administrator to reset the password. Windows also provides a security log that documents all login attempts.

Summary

The DeltaV “built for batch” technology simplifies 21 CFR Part 11 compliance with a commercial off-the-shelf (COTS) batch solution. Competitive systems depend upon engineered solutions that require third-party software and non-value-add systems integration services to deliver a solution that was integrated into the DeltaV system from the start.

The DeltaV system as standard product includes such features as: Configuration Audit Trail, Recipe Authorization, Batch Historian, operator actions with **Confirm and Verify**, and electronic operator log for linking operator comments to batches. These features are integrated into the DeltaV system, minimizing any need for custom code or interfaces. The DeltaV fully integrated built-for-batch automation system reduces maintenance/upgrade costs and makes validation easier.

Appendix A–DeltaV Reference Table for Part 11 Compliance

The following table defines key, specific sections of the 21 CFR Part 11 rule and provides an explanation of how DeltaV (v5.3) software supports each of those requirements. DeltaV support for compliance is discussed with reference to: configuration engineering applications, run time applications, and history applications for each Part 11 section.

Part I: Checklist for DeltaV's Configuration Engineering and Run Time Applications

21CFR Sect. 11.10 Subpart B—Electronic Records	Configuration Engineering Application	Run Time Application
Controls for closed systems 11.10 Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:	DeltaV customers are responsible for developing procedures to support the use of the applications in a regulated environment.	DeltaV customers are responsible for developing procedures to support the use of the applications in a regulated environment.
Controls for closed systems 11.10(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Validation of systems: DeltaV customers must validate the applications. Customers may develop and/or execute the validation plans and protocols themselves or outsource these activities. The validation should follow an established system life cycle (SLC) methodology.	Validation of systems: DeltaV customers must validate the applications. Customers may develop and/or execute the validation plans and protocols themselves or outsource these activities. The validation should follow an established system life cycle (SLC) methodology.

21CFR Sect. 11.10 Subpart B – Electronic Records	Configuration Engineering Application	Run Time Application
	Ability to discern invalid or altered records: DeltaV Configuration Audit Trail, when enabled, documents all changes to the system configuration. When the Audit trail feature is not enabled, changes are not tracked. The ability to disable the audit trail feature is controlled by DeltaV security. Imported configurations cannot be imported without being detected by the audit trail. DeltaV Configuration Audit Trail provides both graphical and textual view of differences between configuration objects.	Ability to discern invalid or altered records: Electronic Operator Log allows comments to be attached to records, but there is no mechanism to over write or replace a record
11.10(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency.	Configuration applications (Explorer, Control Studio, Recipe Studio, etc.) allow viewing of all DeltaV configuration items All configuration data may be printed from the configuration applications Configuration audit trail information may also be viewed on-line and printed	Not applicable

21CFR Sect. 11.10 Subpart B – Electronic Records	Configuration Engineering Application	Run Time Application
11.10(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Built-in security, controls access to DeltaV configuration applications and database administration tools Complete set of database administration tools that facilitate DB backup, restore, etc. Configuration audit trail provides version tracking and supports item recovery and rollback Customers should establish policies and procedures to ensure that records are retained for an appropriate duration of time	Not applicable
11.10(d) Limiting system access to authorized individuals	Sophisticated security system that is layered on Windows security. Uses function locks and keys. Username / password. Access controlled by function & plant area Data files created with read-only access	Sophisticated security system that is layered on Windows security. Uses function locks and keys. Username / password. Access controlled by function & plant area Operator confirmation and verifier approval options available in run time environment

21CFR Sect. 11.10 Subpart B – Electronic Records	Configuration Engineering Application	Run Time Application
11.10(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying	Configuration audit trail tracks who, where, when and what Provides comprehensive version management and change tracking Version to version "differences" can be viewed on line and printed Provides the ability to rollback and restore previous versions of a configuration item	All Operator actions are recorded in a secure time and date stamped electronic record. Within DeltaV, electronic records are not modified or deleted. Time synchronization is provided for all devices in the system with time resynchronization after disaster recovery.
11.10(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Audit Trail will capture modifications to the DeltaV configuration database, tracking who, where, when, and what	Operator actions from batch operator interface and campaign manager can be configured to require confirmer and verifier authentication Operator prompts can be configured to require confirmer and verifier authentication Operator must have security key(s) for the area the action is being taken in Auto logout after extended period of inactivity

21CFR Sect. 11.10 Subpart B – Electronic Records	Configuration Engineering Application	Run Time Application
11.10(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	DeltaV system provides authority checks to ensure only authorized individuals can use the configuration engineering application. This is enabled via the DeltaV security system.	Operator actions from batch operator interface and campaign manager can be configured to require confirmer and verifier authentication Operator prompts can be configured to require confirmer and verifier authentication Operator must have security key(s) for the area the action is being taken in
11.10(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Only DeltaV terminals can enter data and take control actions. The system enforces validity checks since a device must be downloaded from the DeltaV engineering stations to become a valid device. Customer is responsible for non-DeltaV devices	Only DeltaV terminals can enter data and take control actions. The system enforces validity checks since a device must be downloaded from the DeltaV engineering stations to become a valid device.

21CFR Sect. 11.10 Subpart B – Electronic Records	Configuration Engineering Application	Run Time Application
11.10(i) Determine that persons who develop, maintain, or use electronic signature systems have the education, training, and experience to perform their assigned tasks.	DeltaV customers are responsible for ensuring that all persons involved with regulated system have the necessary levels of education, training, and experience to perform their assigned tasks.	DeltaV customers are responsible for ensuring that all persons involved with regulated system have the necessary levels of education, training, and experience to perform their assigned tasks.
11.10(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	DeltaV customers are responsible for developing policies and procedures to support the use of the applications in a regulated environment.	DeltaV customers are responsible for developing policies and procedures to support the use of the applications in a regulated environment.
11.10(k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance	Protection of records Full support for archival of configuration change histories Limiting access DeltaV security with lock and key system	Not applicable
11.10(k) (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	The DeltaV configuration engineering application provides automatic version control for all engineering changes. All changes are stamped with new versions including time and date of changes and who made the change. Version identifier downloaded to controllers (modules) and batch executive (recipes)	Not applicable

21CFR Sect. 11.30 Controls for Open Systems	Configuration Engineering Application	Run Time Application
Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ additional controls such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	Not applicable. The DeltaV system is a closed system.	Not applicable. The DeltaV system is a closed system.

21CFR Sect. 11.50 Signature Manifestations	Configuration Engineering Application	Run Time Application
a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (1) printed name of the signer (2) date and time when the signature was executed (3) the meaning associated with the signature	Include name of signer (username) as well as complete name if available All historical data records include date and time stamps Separate signatures and security keys for “confirmers” and “verifiers”	Include name of signer (username) as well as complete name if available All historical data records include date and time stamps Separate signatures and security keys for “confirmers” and “verifiers”
11.50 (b) The items identified in paragraphs (a)(1), (a)(2) and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	Not applicable—this only restates that the same requirements, listed earlier, should be applied to electronic signatures.	Not applicable—this only restates that the same requirements, listed earlier, should be applied to electronic signatures

21CFR Sect. 11.70 Signature/Record Linking	Configuration Engineering Application	Run Time Application
That electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copies or otherwise transferred so as to falsify an electronic record by ordinary means.	Electronic signatures are integral part of batch history DeltaV data view and analysis tools do not provide any mechanism to allow the modification or deletion of a record	Electronic signatures are integral part of batch history DeltaV data view and analysis tools do not provide any mechanism to allow the modification or deletion of a record

21CFR Sect. 11.100 Subpart C--Electronic Signatures	Configuration Engineering Application	Run Time Application
11.100 General Requirements (a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	DeltaV customers in FDA-regulated environments must be responsible for ensuring that electronic signatures are unique to one individual and not reused by or reassigned to any other individual. DeltaV security is centralized--one security database is used for the entire system. User has the ability to set minimum password lengths and expiration periods Users may be prevented from logging in after a predetermined number of failed login attempts DeltaV tracks includes the name of the logged in user as well as the complete name of the user if available	DeltaV customers in FDA-regulated environments must be responsible for ensuring that electronic signatures are unique to one individual and not reused by or reassigned to any other individual. DeltaV security is centralized--one security database is used for the entire system. User has the ability to set minimum password lengths and expiration periods Users may be prevented from logging in after a predetermined number of failed login attempts DeltaV tracks includes the name of the logged in user as well as the complete name of the user if available

21CFR Sect. 11.100 Subpart C--Electronic Signatures	Configuration Engineering Application	Run Time Application
(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	DeltaV customers in FDA-regulated environments must be responsible for verifying the identities of individuals using electronic signatures.	DeltaV customers in FDA-regulated environments must be responsible for verifying the identities of individuals using electronic signatures.
(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.	DeltaV customers in FDA-regulated environments must be responsible for certifying to the agency that the electronic signatures in their system are intended to be the legally binding equivalent of traditional handwritten signatures.	DeltaV customers in FDA-regulated environments must be responsible for certifying to the agency that the electronic signatures in their system are intended to be the legally binding equivalent of traditional handwritten signatures.
(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.	DeltaV customers must be responsible for certifying to the agency that the electronic signatures in their system are intended to be the legally binding equivalent of traditional handwritten signatures.	DeltaV customers must be responsible for certifying to the agency that the electronic signatures in their system are intended to be the legally binding equivalent of traditional handwritten signatures.
(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	DeltaV customers must be responsible for certifying to the agency that the electronic signatures in their system are intended to be the legally binding equivalent of traditional handwritten signatures.	DeltaV customers must be responsible for certifying to the agency that the electronic signatures in their system are intended to be the legally binding equivalent of traditional handwritten signatures.

21CFR Sect. 11.200 Subpart C--Electronic Signatures	Configuration Engineering Application	Run Time Application
11.200 Electronic signature components and controls (a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password.	DeltaV utilizes username and password entry Confirmer field is pre-populated with the username of the current DeltaV user Confirmer can be changed to allow other users to take action at stations where they are not logged on Verifier approval field is never pre-populated Passwords are never displayed and are not accessible by any user	DeltaV utilizes username and password entry Confirmer field is pre-populated with the username of the current DeltaV user Confirmer can be changed to allow other users to take action at stations where they are not logged on Verifier approval field is never pre-populated Passwords are never displayed and are not accessible by any user

21CFR Sect. 11.200 Subpart C--Electronic Signatures	Configuration Engineering Application	Run Time Application
(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.	If the user has logged off the system	Confirm and verify signature feature (when enabled) may require sign off with user name and password for operator actions through the batch operator interface and campaign manager. Confirmer field is pre-populated with the username of the current DeltaV user Confirmer can be changed to allow other users to take action at stations where they are not logged on Verifier approval field is never pre-populated Passwords are never displayed and are not accessible by any user

21CFR Sect. 11.200 Subpart C--Electronic Signatures	Configuration Engineering Application	Run Time Application
(2) Be used only by their genuine owners; and	DeltaV customers are responsible for ensuring that non-biometric electronic signatures are used only by their genuine owners.	DeltaV customers are responsible for ensuring that non-biometric electronic signatures are used only by their genuine owners.
(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.	DeltaV customers are responsible for ensuring compliance	DeltaV customers are responsible for ensuring compliance
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than genuine owners.	Biometric devices are available from 3rd party vendors. Customers are responsible for ensuring compliance.	Biometric devices are available from 3rd party vendors. Customers are responsible for ensuring compliance.

21CFR Sect. 11.300 Subpart C--Electronic Signatures	Configuration Engineering Application	Run Time Application
11.300 Controls for identification codes/passwords Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:		
(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	DeltaV security layered on Windows security Windows security policies allow for uniqueness of each user ID and password combination Users may be locked out a users after a predefined number login failures Security audit logs Domain support is provided in the DeltaV system.	DeltaV security layered on Windows security Windows policies allow for uniqueness of each user ID and password combination Users may be locked out a users after a predefined number login failures Security audit logs Domain support is provided in the DeltaV system.
(b) Ensuring that identification code and password issuances are periodically checked, recalled or revised (e.g. to cover password such events as password aging).	DeltaV system security is based on Windows security, and can be configured to expire passwords on a periodic basis Standard Windows security allows the ability to set a specific number of attempts before the user is locked out of the system. This can be applied to both the NT login and DeltaV logins. This does not apply to the confirm/verify actions as these take place after the user has successfully logged in.	DeltaV system security is based on Windows security, and can be configured to expire passwords on a periodic basis Standard Windows security allows the ability to set a specific number of attempts before the user is locked out of the system. This can be applied to both the Windows login and DeltaV logins. This does not apply to the confirm/verify actions as these take place after the user has successfully logged in.

21CFR Sect. 11.300 Subpart C--Electronic Signatures	Configuration Engineering Application	Run Time Application
(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	DeltaV customers are responsible for employing controls to ensure the security and integrity of identification codes and passwords.	DeltaV customers are responsible for employing controls to ensure the security and integrity of identification codes and passwords.
(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	DeltaV system security is based on Windows security, and can be configured to expire passwords on a periodic basis Standard Windows security allows the ability to set a specific number of attempts before the user is locked out of the system. This can be applied to both the Windows login and DeltaV logins. This does not apply to the confirm/verify actions as these take place after the user has successfully logged in.	DeltaV system security is based on Windows security, and can be configured to expire passwords on a periodic basis Standard Windows security allows the ability to set a specific number of attempts before the user is locked out of the system. This can be applied to both the login and DeltaV logins. This does not apply to the confirm/verify actions as these take place after the user has successfully logged in.
(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	Customers are responsible for ensuring compliance.	Customers are responsible for ensuring compliance.

Part II: Checklist for DeltaV History Application

21CFR Sect. 11.10 Subpart B – Electronic Records	History Application
Controls for closed systems 11.10 Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:	DeltaV customers are responsible for developing procedures to support the use of the applications in a regulated environment.
Controls for closed systems 11.10(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Validation of systems: DeltaV customers must validate the applications. Customers may develop and/or execute the validation plans and protocols themselves or outsource these activities. The validation should follow an established system life cycle (SLC) methodology. Ability to discern invalid or altered records: The historical data files are write-protected with write access being given only to the DeltaV applications that need to write data to these files. As such, it is not possible for a user who does not have system administrator privileges to make modifications to the file. DeltaV Flexlock provides a mechanism to prevent DeltaV users' having access to the Windows desktop (i.e. a DeltaV database only account.). Historical data viewing and analysis tools do not provide any mechanism to modify or delete data Electronic Operator Log allows comments to be attached to records, but there is no mechanism to overwrite or replace a record All historical data files are write-protected Audit trail of all actions taken through the Batch Historian administrator interface Cannot prevent sabotage by privileged users.

21CFR Sect. 11.10 Subpart B – Electronic Records	History Application
11.10(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency.	Batch data stored in SQL database - reports created using standard programming tools including Microsoft Visual Basic Batch history view supports electronic viewing and printing of data. Continuous history is stored in a PI proprietary database. This information is available from the Process History View client. This can be displayed and printed. Applications to move data into other environments for analysis (e.g. Access, Excel)
11.10(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Built-in security, controls access to historical data Data archival support for both continuous and batch data Batch Historian administrator tool does not allow for the deletion of a batch history that has not been archived Ability to “re-import” previously archived data Customers should establish policies and procedures to ensure that records are retained for duration of an appropriate time.
11.10(d) Limiting system access to authorized individuals	Sophisticated security system that is layered onto Windows security. Uses function locks and keys. Username / password. Access controlled by function & plant area Data files created with read-only access

21CFR Sect. 11.10 Subpart B – Electronic Records	History Application
11.10(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying	The Batch Historian is the secure data repository for long-term storage of the time and date stamped events generated by the batch executive. Batch Historian will collect the secure, time and date stamped history of all operator and alarms events. All historical files are write protected No provisions in the DeltaV system to change or delete historical records Operator comments are linked to existing record Audit trail of all actions taken through the Batch Historian interface
11.10(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Not applicable
11.10(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	DeltaV system provides authority checks to ensure that only authorized individuals can use the batch history and continuous historian applications. The DeltaV system provides no access to modify data by anyone with any level of security access. Batch history data may be deleted from the system only after they have been archived

21CFR Sect. 11.10 Subpart B – Electronic Records	History Application
11.10(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Only DeltaV terminals can enter data and take control actions. The system enforces validity checks since a device must be downloaded from the DeltaV engineering stations to become a valid device.
11.10(i) Determine that persons who develop, maintain, or use electronic signature systems have the education, training, and experience to perform their assigned tasks.	DeltaV customers are responsible for ensuring that all persons involved with regulated system have the necessary levels of education, training, and experience to perform their assigned tasks.
11.10(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	DeltaV customers are responsible for developing policies and procedures to support the use of the applications in a regulated environment.
11.10(k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance	Not applicable
11.10(k) (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Not applicable

21CFR Sect. 11.30 Controls for Open Systems	History Application
Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ additional controls such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	Not applicable. DeltaV is a closed system

21CFR Sect. 11.50 Signature Manifestations	History Application
11.50 (a) a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (1) printed name of the signer (2) date and time when the signature was executed (3) the meaning associated with the signature	Include name of signer (username) as well as complete name if available All historical data records include date and time stamps Separate signatures and security keys for “confirmers” and “verifiers”
11.50 (b) The items identified in paragraphs (a)(1), (a)(2) and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	Not applicable – this only restates that the same requirements, listed earlier, should be applied to electronic signatures.

21CFR Sect. 11.70 Signature/Record Linking	History Application
That electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copies or otherwise transferred so as to falsify an electronic record by ordinary means.	Electronic signatures are integral part of batch history DeltaV data view and analysis tools do not provide any mechanism to allow the modification or deletion of a record

21CFR Sect. 11.100 Subpart C--Electronic Signatures	History Application
11.100 General Requirements (a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	DeltaV customers in FDA-regulated environments must be responsible for ensuring that electronic signatures are unique to one individual and not reused by or reassigned to any other individual. DeltaV security is centralized--one security database is used for the entire system. User has the ability to set minimum password lengths and expiration periods Users may be prevented from logging in after a predetermined number of failed login attempts DeltaV tracks includes the name of the logged in user as well as the complete name of the user if available
(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	DeltaV customers in FDA-regulated environments must be responsible for verifying the identities of individuals using electronic signatures
(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.	DeltaV customers in FDA-regulated environments must be responsible for verifying the identities of individuals using electronic signatures

21CFR Sect. 11.100 Subpart C--Electronic Signatures	History Application
(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.	DeltaV customers must be responsible for certifying to the agency that the electronic signatures in their system are intended to be the legally binding equivalent of traditional handwritten signatures.
(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	DeltaV customers must be responsible for certifying to the agency that the electronic signatures in their system are intended to be the legally binding equivalent of traditional handwritten signatures.

21CFR Sect. 11.200 Subpart C--Electronic Signatures	History Application
11.200 Electronic signature components and controls (a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password.	DeltaV system uses username and password entry Confirmer field is pre-populated with the username of the current DeltaV user Confirmer can be changed to allow other users to take action at stations where they are not logged on Verifier approval field is never pre-populated Passwords are never displayed and are not accessible by any user
(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.	Not applicable
(2) Be used only by their genuine owners; and	DeltaV customers are responsible for ensuring that non-biometric electronic signatures are used only by their genuine owners.

21CFR Sect. 11.200 Subpart C--Electronic Signatures	History Application
(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.	DeltaV customers are responsible for ensuring compliance
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than genuine owners.	Biometric devices are available from 3rd party vendors. Customers are responsible for ensuring compliance.

21CFR Sect. 11.300 Subpart C--Electronic Signatures	History Application
11.300 Controls for identification codes/passwords Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:	
(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	DeltaV security layered on Windows security Windows policies allow for uniqueness of each user ID and password combination Users may be locked out a users after a predefined number login failures Security audit logs Domain support is provided in DeltaV system
(b) Ensuring that identification code and password issuances are periodically checked, recalled or revised (e.g. to cover password such events as password aging).	DeltaV system security is based on Windows security, and can be configured to expire passwords on a periodic basis Standard Windows security allows the ability to set a specific number of attempts before the user is locked out of the system. This can be applied to both the Windows login and DeltaV logins. This does not apply to the confirm/verify actions as these take place after the user has successfully logged in.
(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	DeltaV customers are responsible for employing controls to ensure the security and integrity of identification codes and passwords.

(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	**DeltaV system security is based on Windows security, and can be configured to expire passwords on a periodic basis** **Standard Windows security allows the ability to set a specific number of attempts before the user is locked out of the system. This can be applied to both the Windows login and DeltaV logins. This does not apply to the confirm/verify actions as these take place after the user has successfully logged in.**

21CFR Sect. 11.300 **Subpart C--Electronic Signatures**	**History Application**
(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	**Customers are responsible for ensuring compliance.**