

DeltaV™ Capabilities for Electronic Records Management and Data Integrity

This paper describes DeltaV's integrated solution for meeting Electronic Records Management and Data Integrity requirements in process automation applications using a configurable off-the-shelf (COTS) solution.

Table of Contents

References 3
Introduction 4
Procedural and Technical Controls..... 4
Integrated Features and Custom Applications..... 5
Aspects of 21 CFR Part 11 5
Subpart B—Electronic Records..... 5
Section 11.10 Controls for Closed Systems..... 5
11.10(a) Altered Records..... 6
11.10(b) Reproduction of Records..... 6
11.10(c) Protection of Records..... 6
11.10(d) Limiting Access to Authorized Individuals..... 7
11.10(e) Audit Trails..... 8
11.10(f) Enforce Permitted Sequencing of Steps and Events.....12
11.10(g) Use of Authority Checks..... 12
11.10(h) Device Checks..... 13
11.10(i) Education, Training, and Experience for System Administrators..... 13
11.10(j) Record and Signature Falsification 13
11.10(k) Control over System Documentation..... 13
11.30 Controls for open systems..... 17
11.50 Signature Manifestations..... 17
11.70 Signature/Record Linking..... 17
Subpart C—Electronic Signatures..... 17
11.200 Electronic Signature Components and Controls..... 17
11.300 Controls for Identification Codes and Passwords..... 18
Aspects of FDA Draft Guidance on Data Integrity.....19
Summary..... 23
Appendix A – DeltaV Reference Table for Part 11 Compliance..... 24
Appendix B – DeltaV Reference Table for Annex 11..... 39
Appendix C – DeltaV Reference Table for MHRA Data Integrity Definitions and Guidance..... 48

References

1. CFR – Code of Federal Regulations Title 21, Part 11 (FDA)
2. EudraLex, The Rules Governing Medicinal Products in the European Union, Volume 4, Good Manufacturing Practice, Medicinal Products for Human and Veterinary Use, Annex 11: Computerised Systems (European Commission, Health and Consumers Directorate-General)
3. Data Integrity and Compliance With CGMP; Guidance for Industry; Draft Guidance (FDA April 2016)
4. MHRA GMP Data Integrity Definitions and Guidance for Industry March 2015 (MHRA)

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 originally 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 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.

Similarly to FDA's 21 CFR Part 11, the European Union's Annex 11 (see References 2) provides guidance for the use of computerized systems within GMP-regulated activities in EU directives. The objective of Annex 11 is to ensure that when a computerized system is used, the same product quality and quality assurance can be achieved as manual systems with no increase in the overall risk. Although Annex 11 is not a regulation, it is a guideline and is key to compliance with GMP principles in EU directives covering human and veterinary medicinal products.

In addition to 21 CFR Part 11 and Annex 11, both FDA and the U.K. Medicines and Healthcare Products Regulatory Agency (MHRA) have recently released guidance on Data Integrity (see References 3 and 4) due to the increasingly observed CGMP violations involving data integrity during CGMP inspections. These guidance are intended to clarify the role and importance of data integrity as it is fundamental in a pharmaceutical quality system to ensure the safety, efficacy, and quality of drugs.

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 Data Integrity and Electronic Records Management requirements for CGMP records. The body of this whitepaper provides an overview of the DeltaV system and how it supports 21 CFR Part 11 compliance and the FDA draft guidance on Data Integrity.

The detailed "rule-by-rule" analysis for 21 CFR Part 11, Annex 11 and MHRA Data Integrity Guidance will be presented in tabular form in Appendix A, B and C respectively.

Procedural and Technical Controls

21 CFR Part 11 and Annex 11 establish the requirements for the technical and procedural controls that must be met by the regulated user if the regulated user chooses to maintain regulated records electronically.

Both the FDA's Part 11 and the European Union's Annex 11 cover the same topic, the use of computerized systems in regulated activities, but with different approach. Part 11 emphasises on the requirements (procedural and technical) that need to be met in order to conform to regulations. Annex 11 emphasises on how to conform to its rules and takes a risk-based quality management approach of computerized systems.

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. This paper will focus on the technical control capabilities of a DeltaV system.

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 and Annex 11 compliance with features such as:

- Version Control and Audit Trail (VCAT)
- Recipe Authorization
- SIS Module Authorization
- SIS Functional Test Recording
- Operator Actions with Confirm/Verify
- Batch Historian
- Continuous Historian
- Operator Electronic Log
- Electronic Signatures

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. Cross references of the applicable 21 CFR Part 11 sections to the corresponding Annex 11 and MHRA Data Integrity Guidance sections will be provided in Appendix B and C.

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 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. Only authorized users will be able to access Windows desktop and perform operating system level tasks.

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 privileges 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 and Microsoft Excel, 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 from having access to the Windows 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.

BatchID	Batch Start Time	Batch UniqueID	Archived In
20040813.184013	8/13/2004 1:44:37 PM	CONNER2_20040813_184345642	<Not Archived>
20040813.183227	8/13/2004 1:32:37 PM	CONNER2_20040813_183231082	<Not Archived>
20040813.181428	8/13/2004 1:14:55 PM	CONNER2_20040813_181445019	<Not Archived>
20040813.153943	8/13/2004 10:54:02 AM	CONNER2_20040813_154002311	<Not Archived>
20040806.201714	8/6/2004 3:17:40 PM	CONNER2_20040806_201733120	<Not Archived>
20040806.200537	8/6/2004 3:05:53 PM	CONNER2_20040806_200548737	<Not Archived>
20040806.195430	8/6/2004 2:54:54 PM	CONNER2_20040806_195449589	BatchArchive
20040806.194828	8/6/2004 2:48:44 PM	CONNER2_20040806_194840388	BatchArchive
20040806.192301	8/6/2004 2:23:20 PM	CONNER2_20040806_192314594	BatchArchive
20040806.190441	8/6/2004 2:05:16 PM	CONNER2_20040806_190456074	BatchArchive
20040806.184904	8/6/2004 1:49:13 PM	CONNER2_20040806_184908973	BatchArchive
20040806.184308	8/6/2004 1:43:38 PM	CONNER2_20040806_184333030	BatchArchive
20040721.194042	7/21/2004 2:40:51 PM	CONNER2_20040721_194046259	<Not Archived>
20040301.034636	2/29/2004 9:46:49 PM	CONNER2_20040301_034642771	<Not Archived>
20040301.034122	2/29/2004 9:41:35 PM	CONNER2_20040301_034127868	<Not Archived>
20040301.033510	2/29/2004 9:35:47 PM	CONNER2_20040301_033516725	<Not Archived>
20040301.033058	2/29/2004 9:31:14 PM	CONNER2_20040301_033107256	<Not Archived>
20040301.032508	2/29/2004 9:25:47 PM	CONNER2_20040301_032512546	<Not Archived>
20040301.031633	2/29/2004 9:16:48 PM	CONNER2_20040301_031639398	<Not Archived>
20040301.030036	2/29/2004 9:00:53 PM	CONNER2_20040301_030040820	<Not Archived>
20040225.222613	2/25/2004 4:26:22 PM	CONNER2_20040225_222617258	<Not Archived>
20040225.213748	2/25/2004 3:38:02 PM	CONNER2_20040225_213754354	<Not Archived>

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. This section also applies to Question 4 (How should access to CGMP computer systems be restricted) of the FDA Draft Guidance on Data Integrity (see References 3).

The DeltaV system has built-in security that controls access to DeltaV configuration applications, database administration tools, and runtime operations. It has a sophisticated security system that is layered on the Microsoft 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, by parameter, and by field.

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.

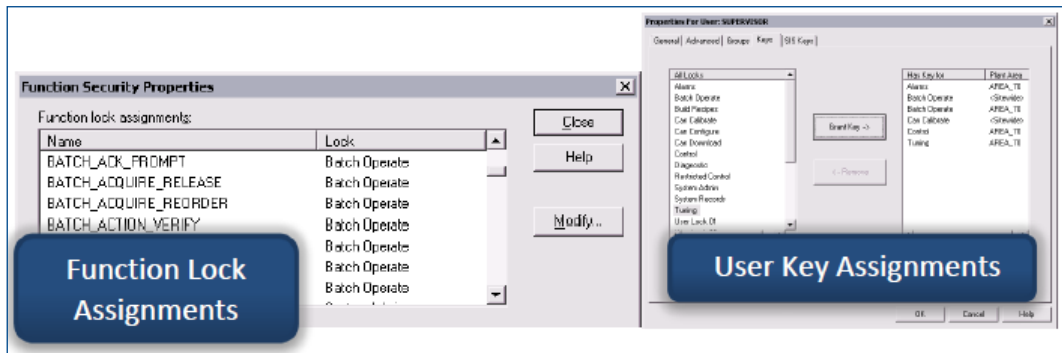


Figure 2 – Single security system for all DeltaV applications controls the level of system access for each user.

In addition, DeltaV Flexlock control user 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. DeltaV Flexlock prevents unauthorized users from accessing the Windows environment and performing tasks such as file deletion or user accounts modification.

A DeltaV system uses Microsoft Remote Desktop to provide remote login capability to a DeltaV Terminal Server. Remote Desktop is initially disabled during the installation of the Windows operating system on DeltaV server and must be explicitly enabled to allow remote login capability.

On the DeltaV Terminal Server machines, DeltaV Explorer allows DeltaV administrator to specify which workstations and users are authorized to establish remote desktop connection with the server. This prevents unauthorized users or workstations from accessing a DeltaV system remotely. Once a remote session is established with a DeltaV Terminal Server, the user will then have access to DeltaV through the FlexLock system based on his/her user privileges.

A DeltaV system supports the use of virtual machines (hosted in Windows server platforms) and thin client workstations to provide the DeltaV virtualization solution. DeltaV Virtual Studio is the integrated application environment that allows a system administrator to manage all the virtual DeltaV system components including the creation of virtual network and start/stop of DeltaV virtual machines.

The networks used to connect thin client workstations to virtual machines are referred to as DeltaV Virtualization Networks. Each DeltaV Virtualization Network must have its own private, independent, IP address space. Only DeltaV virtual machines and DeltaV thin client workstations are allowed to connect to DeltaV Virtualization Networks. The isolation of the DeltaV Virtualization Networks prevent unauthorized access to the DeltaV virtual servers.

The DeltaV Remote Desktop Connection (DRDC) is the mechanism by which an authorized user will connect to a DeltaV virtual machine using a thin client workstation. DRDC adds an additional layer of security on top of the standard RDP protocol. The DeltaV security setting in the virtual environment works the same as in non-virtualized DeltaV architecture. Only authorized users and thin clients will be allowed to connect to the DeltaV virtual machines. As in the traditional DeltaV architecture, once a remote session is established with a DeltaV virtual machines, the user will have access to DeltaV through the FlexLock system based on his/her user privileges.

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 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.

Run Time Application

All operator actions are recorded in a secure time- and date-stamped electronic record. Both old** and new values of the changed parameter are captured during a user change event (does not include changes to the Batch Execute and Historians). Within the DeltaV system, electronic records are not able to be modified or deleted.

** The logging of the old/previous value during a user change event is only available in DeltaV v13.3.1 or later.

Batch History Application

Batch-related events are captured as an electronic record in the Batch Historian and include a time and date stamp, the identity of the person making the entry, 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

BatchID	Batch Start Time	Batch UniqueID	Archived In
20040813.184013	8/13/2004 1:44:37 PM	CONNER2_20040813_184345642	<Not Archived>
20040813.183227	8/13/2004 1:32:37 PM	CONNER2_20040813_183231082	<Not Archived>
20040813.181428	8/13/2004 1:14:55 PM	CONNER2_20040813_181445019	<Not Archived>
20040813.153943	8/13/2004 10:54:02 AM	CONNER2_20040813_154002311	<Not Archived>
20040806.201714	8/6/2004 3:17:40 PM	CONNER2_20040806_201733120	<Not Archived>
20040806.200537	8/6/2004 3:05:53 PM	CONNER2_20040806_200548737	<Not Archived>
20040806.195430	8/6/2004 2:54:54 PM	CONNER2_20040806_195449589	BatchArchive
20040806.194828	8/6/2004 2:48:44 PM	CONNER2_20040806_194840388	BatchArchive
20040806.192301	8/6/2004 2:23:20 PM	CONNER2_20040806_192314594	BatchArchive
20040806.190441	8/6/2004 2:05:16 PM	CONNER2_20040806_190456074	BatchArchive
20040806.184904	8/6/2004 1:49:13 PM	CONNER2_20040806_184908973	BatchArchive
20040806.184308	8/6/2004 1:43:38 PM	CONNER2_20040806_184333030	BatchArchive
20040721.194042	7/21/2004 2:40:51 PM	CONNER2_20040721_194046259	<Not Archived>
20040301.034636	2/29/2004 9:46:49 PM	CONNER2_20040301_034642771	<Not Archived>
20040301.034122	2/29/2004 9:41:35 PM	CONNER2_20040301_034127868	<Not Archived>
20040301.033510	2/29/2004 9:35:47 PM	CONNER2_20040301_033516725	<Not Archived>
20040301.033058	2/29/2004 9:31:14 PM	CONNER2_20040301_033107256	<Not Archived>
20040301.032508	2/29/2004 9:25:47 PM	CONNER2_20040301_032512546	<Not Archived>
20040301.031633	2/29/2004 9:16:48 PM	CONNER2_20040301_031639398	<Not Archived>
20040301.030036	2/29/2004 9:00:53 PM	CONNER2_20040301_030040820	<Not Archived>
20040225.222613	2/25/2004 4:26:22 PM	CONNER2_20040225_222617258	<Not Archived>
20040225.213748	2/25/2004 3:38:02 PM	CONNER2_20040225_213754354	<Not Archived>

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

Historian Administrator that documents any time events are deleted after they have been archived by users with the proper access privilege.

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
System Admin Activities	
Security	
Define Valid Users	Windows Security Log and DeltaV Version Control and Audit Trail
History Archiving	Batch Historian Administrator Tool
Operations	
Operator Actions	DeltaV Event Journal Both old and new values of the changed parameter are captured during a user change event <i>Note: The logging of the old/previous value during a user change event is only available in DeltaV v13.3.1 or later.</i>
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/Hold/Restart/Abort Procedure	Batch Historian
Start/Stop/Hold/Restart/Abort Unit Procedure	Batch Historian
Start/Stop/Hold/Restart/Abort Operation	Batch Historian
Start/Stop/Hold/Restart/Abort Phase	Batch Historian
Operator prompts	Batch Historian
Operator prompt response	Batch Historian
Equipment Selections	Batch Historian
Operator Actions to the Batch	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 and Equipment Modules (including SIS Modules)	DeltaV Version Control and Audit Trail
Equipment and Control Module Classes	DeltaV Version Control and Audit Trail

Item	Audit Trail Implementation
Named Sets	DeltaV Version Control and Audit Trail
Equipment Trains	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
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
Recipe Parameters	DeltaV Version Control and Audit Trail
Report Parameters	DeltaV Version Control and Audit Trail
Unit Parameters	DeltaV Version Control and Audit Trail
Unit Selection Policies	DeltaV Version Control and Audit Trail
Operator Displays	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
Alarm Help	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

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 will be tracked and allowed only by personnel with the appropriate authorization.

Authorized personnel can configure the DeltaV Batch Operator Interface, Campaign Manager Operator Interface, DeltaV Operate and Control Studio online 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.

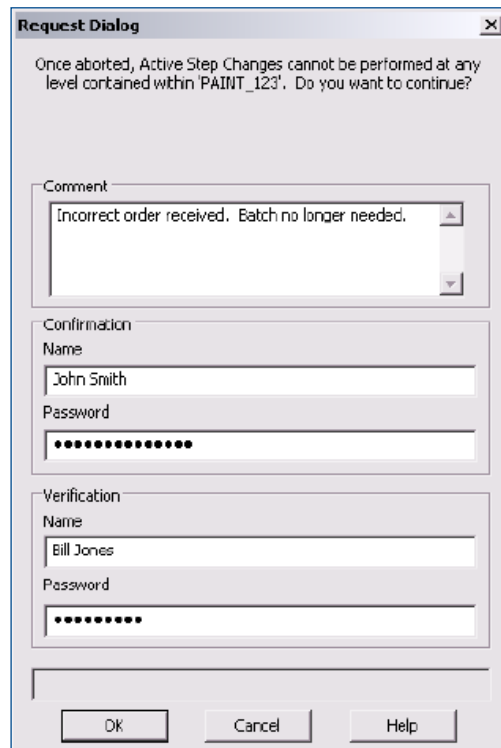
11.10(g) Use of Authority Checks

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 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 from having access to the Windows desktop or a DeltaV database account.

Run Time Application: Operator actions from DeltaV Operate, Control Studio online, the Batch Operator Interface and Campaign Manager Operator Interface 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.



The screenshot shows a 'Request Dialog' window with the following content:

Once aborted, Active Step Changes cannot be performed at any level contained within 'PAINT_123'. Do you want to continue?

Comment
Incorrect order received. Batch no longer needed.

Confirmation
Name: John Smith
Password: [masked]

Verification
Name: Bill Jones
Password: [masked]

Buttons: OK, Cancel, Help

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. A 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.

11.10(h) Device Checks

Section 11.10(h) concerns the “...*Use of device (e.g. terminal) 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. All DeltaV workstations, controllers, and I/O devices must be defined in the DeltaV Explorer and downloaded before they can participate in DeltaV communications. Devices connected to the DeltaV system that are not configured in the DeltaV Explorer are not recognized by the DeltaV system and are not allowed to participate in DeltaV communications.

System users with proper security privileges 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(j) Record and Signature Falsification

Section 11.10(j) requires that “*written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification*” be established and adhered to. It is the customer’s responsibility to ensure that such policies and procedures are developed and followed in order to support the use of the applications in a regulated environment.

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. Check out of control configuration (control modules, unit modules, procedures, unit procedures, operations, etc.) to an authorized user is automatically enforced before any changes can be made.

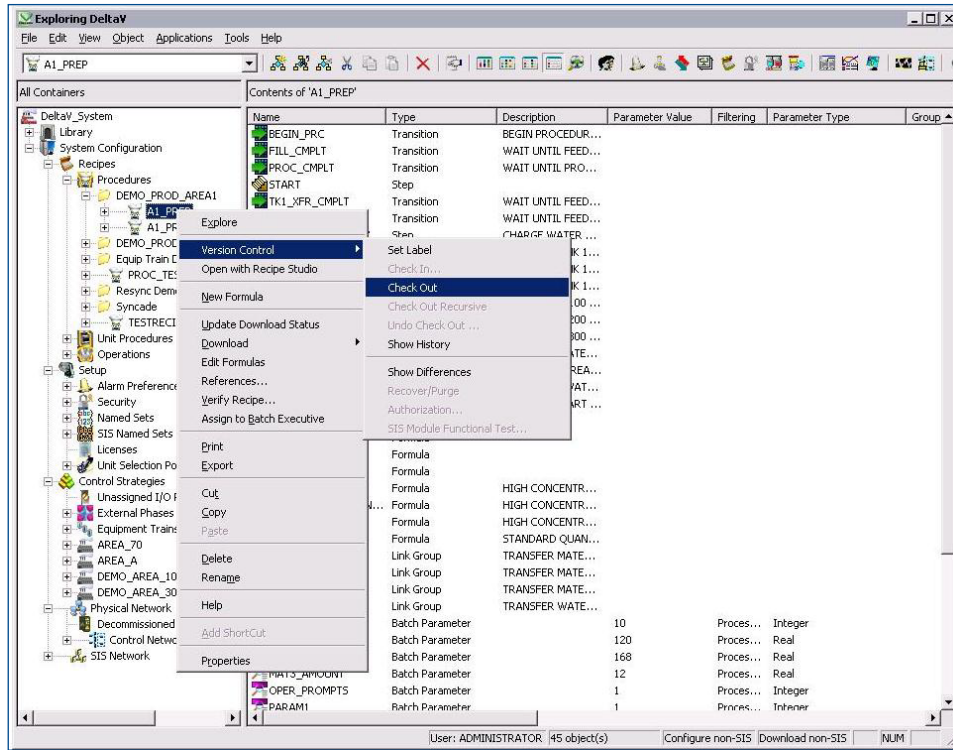


Figure 5 – DeltaV Explorer provides visual indication that a Module is checked out for changes.

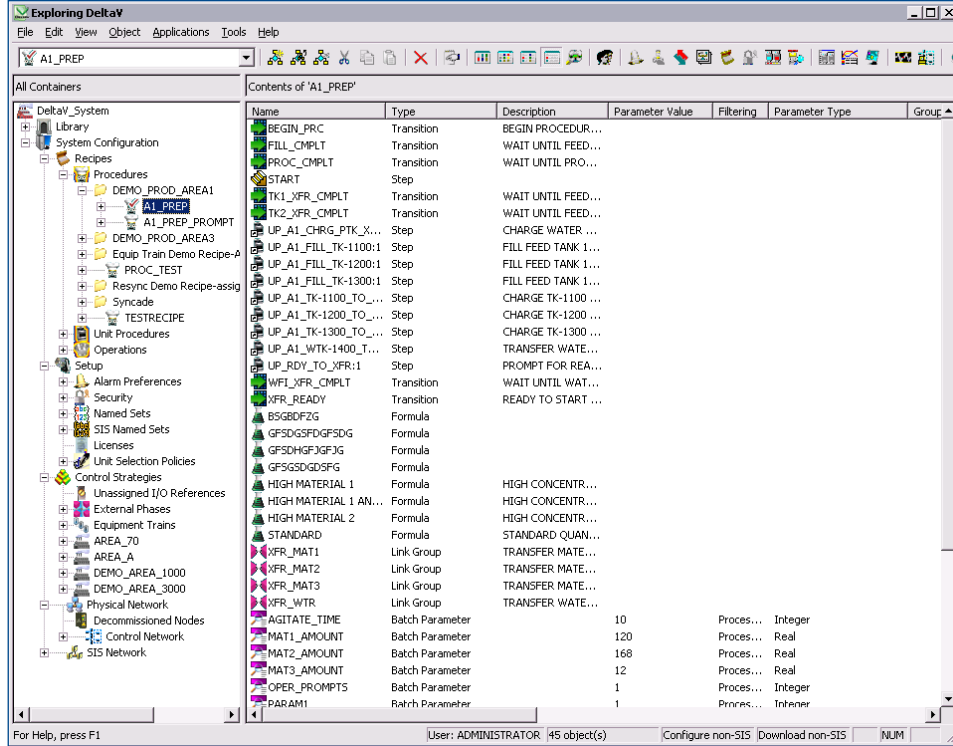


Figure 6 – Module checkout for Version Control and Audit Trail.

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.

Version	User	Date	Action	Archive Stat
1	Administrator	4/15/2011 3:01:32 PM	Undo Checkout	None
1	Administrator	4/15/2011 2:58:01 PM	Checked Out	None
1	Administrator	4/15/2011 2:44:58 PM	Download Label: sent to USAUST-MKTG008	None
1	Administrator	4/15/2011 9:27:54 AM	Download Label: sent to USAUST-MKTG008	None
1	ADMINISTRATOR	4/15/2011 9:10:41 AM	Label: Upgrade Completed	None
1	ADMINISTRATOR	4/15/2011 9:10:41 AM	Label: Enabled Version Control	None
1 (U)	ADMINISTRATOR	4/15/2011 9:09:14 AM	Checked In - Due to Upgrade	None
0	ADMINISTRATOR	4/15/2011 9:09:13 AM	Checked Out - Due to Upgrade	None
0	ADMINISTRATOR	4/15/2011 9:09:13 AM	Created	None

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

The DeltaV Configuration 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.

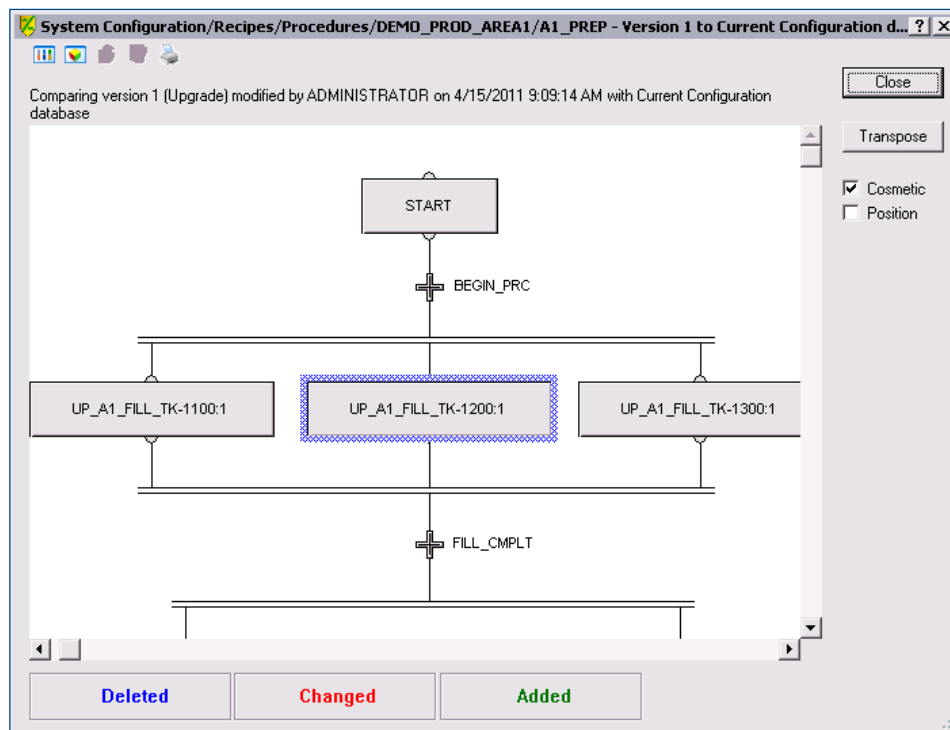


Figure 8 – Difference reports may be generated between any two versions. Graphical difference report indicates what has been deleted, added, or changed.

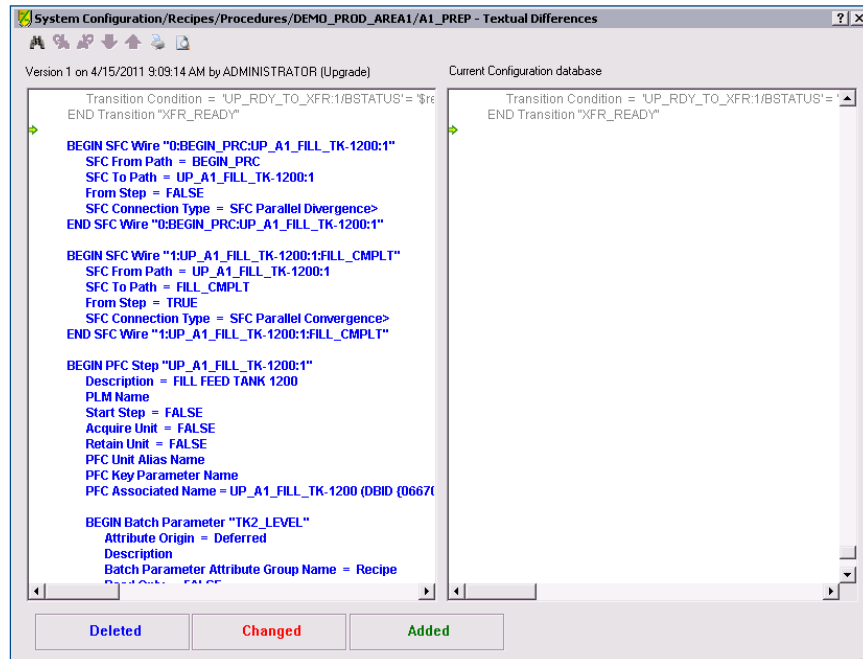


Figure 9 – Change report shown in text view.

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.

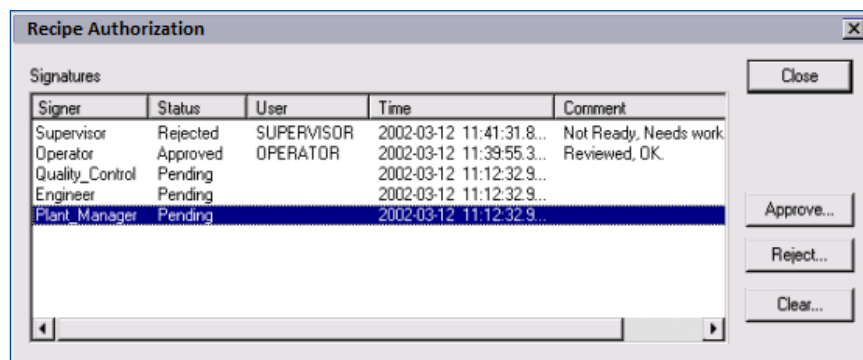


Figure 10 – Recipe authorization may require from one to five user approvals before a recipe can be downloaded.

SIS Module Authorization and Functional Test Recording: Similar to the recipe authorization feature, SIS module authorization may allow from one to five user approvals before an SIS module may be released to production for use. A separate user approval list can be set up for each the SIS modules. Just like with recipe authorization, the SIS module authorization is tightly integrated with the Configuration Audit Trail and Version Management to track module changes, approvals, and comments. Unapproved SIS modules cannot be downloaded.

Likewise, when SIS module functional test recording is enabled, up to five electronic signatures may be configured to be required before an SIS module function test is approved. A record will be entered in the Configuration Audit Trail database when the function tests have been successfully completed.

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).

To further clarify the meaning of the signing in addition to Confirm/Verify, a DeltaV system allows an operator to enter a comment about the parameter change. By default, the DeltaV system concatenates the string "VALUE SIGNED FOR = ", the value of the parameter entered, and the operator comment as one event and stores it as a historical data record.

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. Signatures cannot be copied, transferred or falsified. The 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, Control Studio online, the Batch Operator Interface and Campaign Manager Operator Interface 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 ID and passwords are lost or compromised, and that safeguards be in place to detect and prevent unauthorized use of user IDs and passwords.

Since DeltaV user IDs and passwords are part of the Windows security system, they have available the full functionality of the Windows security system that enforces unique user IDs 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.

Aspects of FDA Draft Guidance on Data Integrity

The FDA Data Integrity Guidance (see References 2) is a draft guidance that provides the FDA’s current thinking on the creation and handling of data in accordance with CGMP requirements. It is a Q&A style guidance focused on frequently occurring data integrity lapses with definition of key terms.

Data integrity refers to maintaining and assuring the accuracy and consistency of data over its entire life-cycle. It is a critical aspect to the design, implementation and usage of any system which stores, processes or retrieves data. The integrity of the data collected and recorded by pharmaceutical manufacturers is critical to ensuring that high quality and safe medicines are produced. Breaches in data integrity can have significant consequences and may lead to patient injury, or even death.

Computerized systems used in regulated industries must ensure that data, irrespective of the format in which it is generated, is recorded, processed, retained and used to ensure a complete, consistent and accurate record throughout the data lifecycle.

This section reviews the questions listed in the FDA Draft Guidance on Data Integrity that are applicable to a DeltaV operation.

The following diagram provides a reference of the relevant DeltaV systems (physical and logical) and the transfer of data between system components.

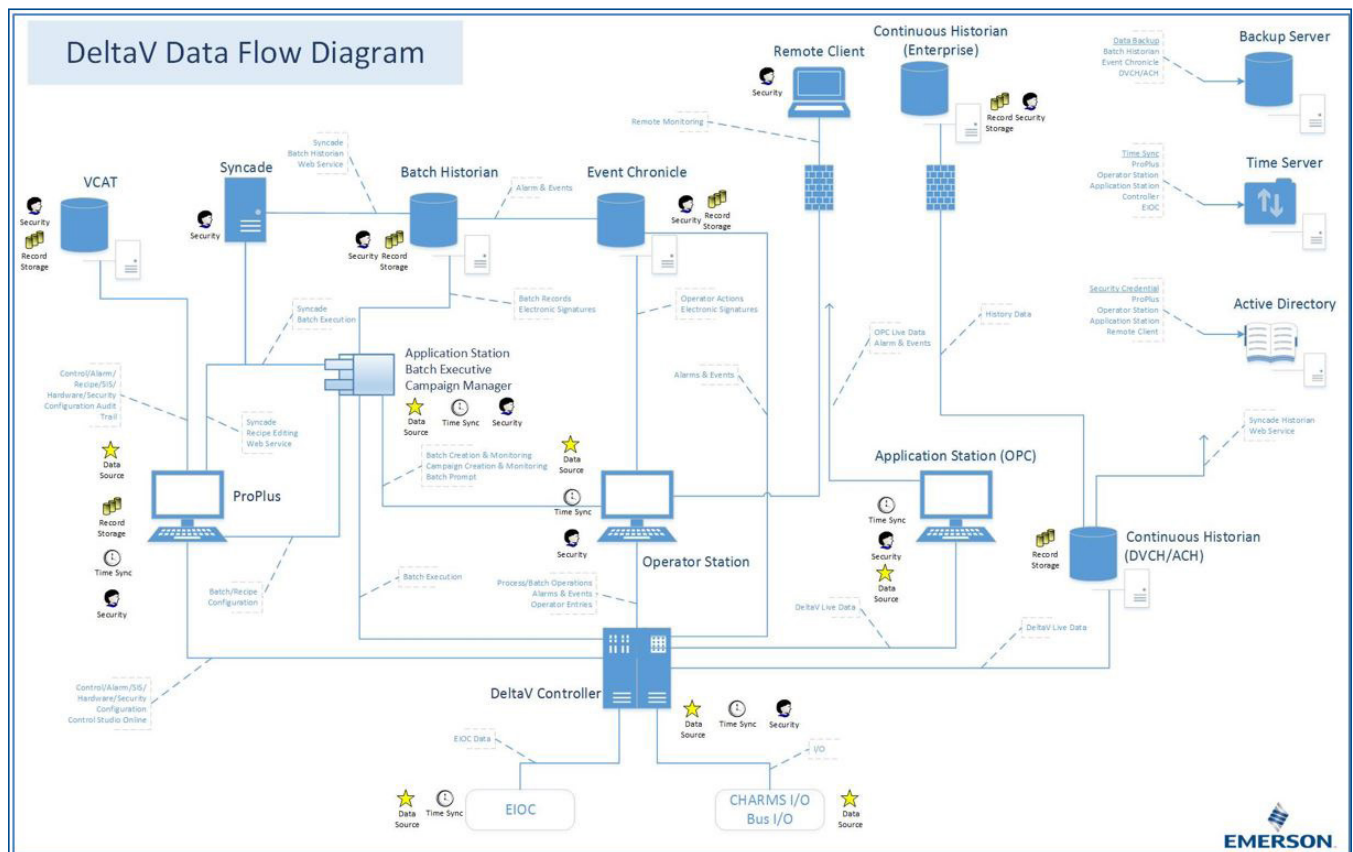


Figure 11 – DeltaV Data Flow Diagram

Question 1a: What is “data integrity”?

The draft guidance stated data integrity refers to the completeness, consistency, and accuracy of data. Complete, consistent, and accurate data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate (ALCOA).

- A – attributable to the person generating the data.
 - ▶ Engineering revisions and changes can be tracked as changes are made using the DeltaV Configuration Audit Trail application. 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.
 - ▶ All operator actions are recorded in a secure time- and date-stamped electronic record with the identity of the operator. Both old and new values of the changed parameter are captured during a user change event.
 - ▶ Batch-related events are captured as an electronic record in the Batch Historian and include a time and date stamp, the identity of the person making the entry, and the location from which the change was made.
- L – legible and permanent.
 - ▶ All configuration and historical data files are stored in secured data repository with write-access given only to the applications that need to write data to those files.
 - ▶ Historical data may be deleted from the system only after they have been archived. This ensures data are stored permanently and protect against accidental deletion of data.
 - ▶ 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 native DeltaV file and database formats, or can be exported in different file formats including text, Microsoft Word and Microsoft Excel for viewing and reporting purpose.
- C – contemporaneous.
 - ▶ All configuration and operator actions are recorded at the time the work is performed with a time and date stamp, the identity of the person making the entry, and the location from which the change was made.
- O – original record or true copy.
 - ▶ The validity of the source of DeltaV data input is restricted to DeltaV devices only. All DeltaV workstations, controllers, and I/O devices must be defined in the DeltaV Explorer and downloaded before they can generate, enter, record and process data in DeltaV. Devices connected to the DeltaV system that are not configured in the DeltaV Explorer are not recognized by the DeltaV system and are not allowed to participate in DeltaV communication.
 - ▶ All configuration and historical data files are stored in its original format in secured data repository. Historical data can only be deleted from the system after they have been archived to ensure a true copy of the original data is maintained securely throughout the records retention period.
- A – accurate.
 - ▶ Built-in security controls access to configuration, operation and historical data to protect against data falsification.
 - ▶ Comprehensive version management and change tracking, including the ability to log all operator actions with old and new values of the changed parameter ensure all data changes are recorded and data accuracy and consistency is maintained throughout the data lifecycle.

Question 1c: What is “audit trail”?

The draft guidance stated audit trail means a secure, computer-generated, time-stamped electronic record that allows for reconstruction of the course of events relating to the creation, modification, or deletion of an electronic record.

The DeltaV system provides audit trails functionalities in the Configuration, Run Time, and History environments:

Configuration Application

Engineering revisions and changes can be tracked as changes are made using the DeltaV Configuration Audit Trail application. This application creates and maintains a complete 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.

Run Time Application

All operator actions are recorded in a secure time- and date-stamped electronic record. Both old and new values of the changed parameter are captured during a user change event.

History Application

Batch-related events are captured as an electronic record in the Batch Historian and include a time and date stamp, the identity of the person making the entry, and the location from which the change was made.

Question 4: How should access to CGMP computer system be restricted?

The draft guidance stated that controls must be exercised to assure that changes to computerized records can be made only by authorized personnel.

The DeltaV system provides authority checks to ensure only authorized individuals can access to DeltaV configuration applications, database administration tools, and runtime operations. The security system is layered on the Windows security system and 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.

In addition, DeltaV Flexlock controls user access to the Windows operating system, Desktop, the DeltaV application and other applications based on user groups as defined by the system administrator. This prevents unauthorized users from doing anything bad in the Windows environment such as file deletion or user accounts modification.

The DeltaV systems uses Microsoft Remote Desktop to provide remote login capability to DeltaV Terminal Server in both the traditional DeltaV architecture and Virtualization environment. Only authorized workstations and users are allowed to establish remote desktop connection with the server. This prevents unauthorized users or workstations to connect remotely. Once a remote session is permitted with a DeltaV Terminal Server, the user will then have access to the system through the DeltaV FlexLock and built-in security system based on his/her user privileges.

The DeltaV system is built upon standard Windows-based software and data management tools that will allow the computer system and data to be accessed and potentially modified by an administrator. Customers should establish policies and procedures to safeguard data. The general approach is to give administrative privileges 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.

Question 5: Why is FDA concerned with the use of shared login accounts for computer systems?

The draft guidance stated that when login credentials are shared, a unique individual cannot be identified through the login and the system would thus not conform to the CGMP requirements.

The use of shared login accounts is strongly discouraged as many operations (configuration and runtime) are logged, sharing accounts makes it difficult to identify the individual that performed an operation by reviewing the DeltaV event and historical log.

As part of the DeltaV installation, a number of built-in user and services accounts are automatically created. We recommend that all built-in accounts created by the DeltaV installation that are not applicable to the system should be removed. And the passwords for all DeltaV built-in accounts should be changed after installation using the DeltaV Security Administration tool.

The DeltaV Service Account (DeltaVAdmin) must exist on all DeltaV workstations in the system and the password for all DeltaVAdmin accounts must be the same to function properly. We recommend that the default password for the DeltaVAdmin account should be changed using the DeltaV ServPwd utility. This utility changes the password for the DeltaV Service account and all the services and components that run as this account.

Question 11: Can electronic signatures be used instead of handwritten signatures for master production and control records?

The draft guidance stated that electronic signatures can be used instead of handwritten signatures when the electronic signatures are able to clearly identify the individual responsible for signing the record and to securely link with the associated record.

Provided the appropriate procedural controls are implemented and enforced, the DeltaV system provides full electronic signature capabilities that clearly identifies the individuals signing the record with the user name, time and date, and meaning of the signing. In addition, DeltaV's electronic signatures are integral part of the batch history and event logs that are securely linked to their respective electronic records. Signatures cannot be copied, transferred or falsified by any means in DeltaV.

These capabilities allow DeltaV's electronic signature to be used instead of handwritten signatures for master production and control records.

Question 12: When does electronic data become a CGMP record?

The draft guidance stated that when electronic data is generated to satisfy a CGMP requirement, all data become a CGMP record.

DeltaV systems provide computer-generated, time and date stamped audit trails records in all DeltaV configuration applications.

All operator actions are recorded in a secure time and date stamped electronic record. Both old** and new values of the changed parameter are captured during a user change event from the controller (does not include changes to the Batch Execute and Historians). Within the DeltaV system, electronic records are not able to be modified or deleted.

The DeltaV Batch Historian is the secure data repository for long-term storage of the time and date stamped events generated by the Batch Executive. All historical records and files in the Batch Historian are write protected and cannot be modified or deleted.

All DeltaV electronic data including audit trail documentation, operation data, and batch records can be used as CGMP records as they are generated to satisfy CGMP requirement.

*** The logging of the old/previous value during a user change event is available in DeltaV v13.3.1 or later.*

Summary

The DeltaV “built for batch” technology simplifies FDA’s 21 CFR Part 11 and EU’s Annex 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, SIS Module Authorization and Functional Test Recording, 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 system 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.

21CFR Sec. 11.10 Subpart B—Electronic Records Controls for Closed Systems	Configuration Engineering Application	Run Time Application	History Application
<p>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:</p>	<p>DeltaV customers are responsible for developing procedures to support the use of the applications in a regulated environment.</p>	<p>DeltaV customers are responsible for developing procedures to support the use of the applications in a regulated environment.</p>	<p>DeltaV customers are responsible for developing procedures to support the use of the applications in a regulated environment.</p>

21CFR Sec. 11.10 Subpart B—Electronic Records Controls for Closed Systems	Configuration Engineering Application	Run Time Application	History Application
<p>11.10(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</p>	<p>Validation of systems:</p> <p>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.</p> <p>Ability to discern invalid or altered records:</p> <p>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.</p> <p>DeltaV Configuration Audit Trail provides both graphical and textual view of differences between configuration objects.</p>	<p>Validation of systems:</p> <p>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.</p> <p>Ability to discern invalid or altered records:</p> <p>Electronic Operator Log allows comments to be attached to records, but there is no mechanism to overwrite or replace a record</p>	<p>Validation of systems:</p> <p>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.</p> <p>Ability to discern invalid or altered records:</p> <p>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 delete historical data files.</p> <p>Historical data viewing and analysis tools do not provide any mechanism to modify or delete data.</p> <p>Electronic Operator Log allows comments to be attached to records, but there is no mechanism to overwrite or replace a record.</p> <p>Audit trail of all actions are taken through the Batch Historian administrator interface</p>

21CFR Sec. 11.10 Subpart B—Electronic Records Controls for Closed Systems	Configuration Engineering Application	Run Time Application	History Application
<p>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.</p>	<p>Configuration applications (Explorer, Control Studio, Recipe Studio, etc.) allow viewing of all DeltaV configuration items.</p> <p>All configuration data may be printed from the configuration applications.</p> <p>Configuration audit trail information may also be viewed on-line and printed.</p>	<p>Not applicable</p>	<p>Batch data stored in SQL database - reports created using standard programming tools including Microsoft Visual Basic.</p> <p>Batch history view supports electronic viewing and printing of data.</p> <p>Continuous history is stored in a proprietary database. This information is available from the Process History View client. This can be displayed and printed.</p> <p>Applications to export data into other environments for analysis (e.g. Access, Excel).</p>
<p>11.10(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.</p>	<p>Built-in security controls access to DeltaV configuration applications and database administration tools.</p> <p>Complete set of database administration tools that facilitate DB backup and restore are available.</p> <p>Configuration audit trail provides version tracking and supports item recovery and rollback.</p> <p>Customers should establish policies and procedures to ensure that records are retained for an appropriate duration of time.</p>	<p>Not applicable</p>	<p>Built-in security controls access to historical data.</p> <p>Data archival support for both continuous and batch data.</p> <p>Batch Historian administrator tool does not allow for the deletion of a batch history that has not been archived.</p> <p>Ability to “re-import” previously archived data.</p> <p>Customers should establish policies and procedures to ensure that records are retained for duration of an appropriate time.</p>

21CFR Sec. 11.10 Subpart B—Electronic Records Controls for Closed Systems	Configuration Engineering Application	Run Time Application	History Application
<p>11.10(d) Limiting system access to authorized individuals</p>	<p>DeltaV built-in security system that is layered on Windows security.</p> <p>Uses the concept of locks and keys to assign system functions, field and parameters to authorized users.</p> <p>Access controlled by function & plant area.</p> <p>Configuration data files created with read-only access.</p> <p>Uses Microsoft Remote Desktop to provide remote login capability to DeltaV Terminal Server. Only specific workstations and users are authorized to establish remote desktop connection with the server. Once a remote session is established with a DeltaV Terminal Server, user will then have access to DeltaV functions based on his/her user privileges.</p> <p>DeltaV Virtualization supports the use of virtual machines and thin client workstations connected to the DeltaV Virtualization Networks. DeltaV Virtualization Networks must be isolated to prevent unauthorized access to the DeltaV virtual servers. DeltaV Remote Desktop Connection is the mechanism by which authorized users will connect to a DeltaV virtual machine using a thin client workstation.</p>	<p>DeltaV built-in security system that is layered on Windows security.</p> <p>Uses the concept of locks and keys to assign system functions, field and parameters to authorized users.</p> <p>Access controlled by function & plant area.</p> <p>Operator confirmation and verifier approval options available in run time environment.</p> <p>Uses Microsoft Remote Desktop to provide remote login capability to DeltaV Terminal Server. Only specific workstations and users are authorized to establish remote desktop connection with the server. Once a remote session is established with a DeltaV Terminal Server, user will then have access to DeltaV functions based on his/her user privileges.</p> <p>DeltaV Virtualization supports the use of virtual machines and thin client workstations connected to the DeltaV Virtualization Networks.</p> <p>DeltaV Virtualization Networks must be isolated to prevent unauthorized access to the DeltaV virtual servers. DeltaV Remote Desktop Connection is the mechanism by which authorized users will connect to a DeltaV virtual machine using a thin client workstation.</p>	<p>DeltaV built-in security system that is layered onto Windows security.</p> <p>Uses the concept of locks and keys to assign system functions, field and parameters to authorized users.</p> <p>Access controlled by function & plant area.</p> <p>Historical data files created with read-only access.</p>

21CFR Sec. 11.10 Subpart B—Electronic Records Controls for Closed Systems	Configuration Engineering Application	Run Time Application	History Application
<p>11.10(e)</p> <p>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.</p>	<p>Configuration audit trail tracks who, where, when and what.</p> <p>Provides comprehensive version management and change tracking.</p> <p>Version to version “differences” can be viewed on line and printed.</p> <p>Provides the ability to rollback and restore previous versions of a configuration item.</p>	<p>All Operator actions are recorded in a secure time and date stamped electronic record. Both old and new values of the changed parameter are captured during a user change event from the controller (does not include changes to the Batch Execute and Historians). Within DeltaV, electronic records are not able to be modified or deleted.</p> <p>Time synchronization is provided for all devices in the system with time resynchronization after disaster recovery.</p> <p><i>Note: The logging of the old/previous value during a user change event is available in DeltaV v13.3.1 or later.</i></p>	<p>The Batch Historian is the secure data repository for long-term storage of the time and date stamped events generated by the Batch Executive.</p> <p>Batch Historian will collect the secure, time and date stamped history of all operator and alarms events.</p> <p>All historical files are write protected</p> <p>No provisions in the DeltaV system to change or delete historical records.</p> <p>Operator comments are linked to existing record.</p> <p>Audit trail of all actions taken through the Batch Historian interface.</p>
<p>11.10(f)</p> <p>Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.</p>	<p>Audit Trail will capture modifications to the DeltaV configuration database, tracking who, where, when, and what.</p>	<p>Operator actions from DeltaV Operate, Control Studio online, the Batch Operator Interface and Campaign Manager Operator Interface can be configured to require confirmer and verifier authentication.</p> <p>Operator prompts can be configured to require confirmer and verifier authentication.</p> <p>Operator must have security key(s) for the area in which the action is being taken.</p> <p>Auto logout after extended period of inactivity.</p>	<p>Not applicable</p>

21CFR Sec. 11.10 Subpart B—Electronic Records Controls for Closed Systems	Configuration Engineering Application	Run Time Application	History Application
<p>11.10(g)</p> <p>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.</p>	<p>DeltaV system provides authority checks to ensure only authorized individuals can use the configuration engineering application. This is enabled via the DeltaV security system.</p>	<p>DeltaV system provides authority checks to ensure that only authorized individuals can perform operator actions from DeltaV Operate, Control Studio online, the Batch Operator Interface and Campaign Manager Operator Interface.</p> <p>All operator actions can be configured to require confirmer and verifier authentication.</p> <p>Operator prompts can be configured to require confirmer and verifier authentication.</p> <p>Operator must have security key(s) for the area in which the action is being taken.</p>	<p>DeltaV system provides authority checks to ensure that only authorized individuals can use the batch history and continuous historian applications.</p> <p>The DeltaV system provides no access to modify data by anyone with any level of security access.</p> <p>Batch history data may be deleted from the system only after they have been archived.</p>
<p>11.10(h)</p> <p>Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.</p>	<p>Only DeltaV terminals can enter data and take control actions.</p> <p>The system enforces validity checks since a device must be defined in the DeltaV Explorer and downloaded from the DeltaV engineering stations to become a valid device.</p> <p>Customer is responsible for non-DeltaV devices.</p>	<p>Only DeltaV terminals can enter data and take control actions.</p> <p>The system enforces validity checks since a device must be defined in the DeltaV Explorer and downloaded from the DeltaV engineering stations to become a valid device.</p>	<p>Only DeltaV terminals can enter data and take control actions.</p> <p>The system enforces validity checks since a device must be defined in the DeltaV Explorer and downloaded from the DeltaV engineering stations to become a valid device.</p>
<p>11.10(i)</p> <p>Determination that persons who develop, maintain, or use electronic signature systems have the education, training, and experience to perform their assigned tasks.</p>	<p>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.</p>	<p>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.</p>	<p>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.</p>

21CFR Sec. 11.10 Subpart B—Electronic Records Controls for Closed Systems	Configuration Engineering Application	Run Time Application	History Application
<p>11.10(j)</p> <p>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.</p>	<p>DeltaV customers are responsible for developing policies and procedures to support the use of the applications in a regulated environment.</p>	<p>DeltaV customers are responsible for developing policies and procedures to support the use of the applications in a regulated environment.</p>	<p>DeltaV customers are responsible for developing policies and procedures to support the use of the applications in a regulated environment.</p>
<p>11.10(k)</p> <p>Use of appropriate controls over systems documentation including:</p> <p>(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.</p> <p>(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.</p>	<p>Protection of records</p> <p>Full support for archival of configuration change histories</p> <p>Limiting access</p> <p>DeltaV security with lock and key system</p> <p>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).</p>	<p>Not applicable</p>	<p>Not applicable</p>

21CFR Sec. 11.30 Controls for Open Systems	Configuration Engineering Application	Run Time Application	History Application
<p>Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ additional controls designed to ensure authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.</p>	<p>Not applicable. The DeltaV system is a closed system.</p>	<p>Not applicable. The DeltaV system is a closed system.</p>	<p>Not applicable. DeltaV is a closed system.</p>

21CFR Sec. 11.50 Signature Manifestations	Configuration Engineering Application	Run Time Application	History Application
<p>11.50(a)</p> <p>Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:</p> <p>(1) The printed name of the signer;</p> <p>(2) The date and time when the signature was executed; and</p> <p>(3) The meaning (such as electronic display or printout) associated with the signature.</p>	<p>Include name of signer (username) as well as complete name if available.</p> <p>All historical data records include date and time stamps.</p> <p>Separate signatures and security keys for “confirmers” and “verifiers.”</p>	<p>Include name of signer (username) as well as complete name if available.</p> <p>All historical data records include date and time stamps.</p> <p>Separate signatures and security keys for “confirmers” and “verifiers”.</p>	<p>Include name of signer (username) as well as complete name if available.</p> <p>All historical data records include date and time stamps.</p> <p>Separate signatures and security keys for “confirmers” and “verifiers”.</p>
<p>11.50 (b)</p> <p>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).</p>	<p>Not applicable—this only restates that the same requirements, listed earlier, should be applied to electronic signatures.</p>	<p>Not applicable—this only restates that the same requirements, listed earlier, should be applied to electronic signatures.</p>	<p>Not applicable – this only restates that the same requirements, listed earlier, should be applied to electronic signatures.</p>

21CFR Sec. 11.70 Signature / Record Linking	Configuration Engineering Application	Run Time Application	History Application
<p>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, copied or otherwise transferred so as to falsify an electronic record by ordinary means.</p>	<p>Electronic signatures are integral part of batch history and event log.</p> <p>DeltaV data view and analysis tools do not provide any mechanism to allow the modification or deletion of a record.</p>	<p>Electronic signatures are integral part of batch history and event log.</p> <p>DeltaV data view and analysis tools do not provide any mechanism to allow the modification or deletion of a record.</p>	<p>Electronic signatures are integral part of batch history and event log.</p> <p>DeltaV data view and analysis tools do not provide any mechanism to allow the modification or deletion of a record.</p>

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

21CFR Sec. 11.100 Subpart C--Electronic Signatures General Requirements	Configuration Engineering Application	Run Time Application	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.	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.	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 Sec. 11.200 Electronic Signature Components and Controls	Configuration Engineering Application	Run Time Application	History Application
<p>11.200</p> <p>(a) Electronic signatures that are not based upon biometrics shall:</p> <p>(1) Employ at least two distinct identification components such as an identification code and password.</p>	<p>DeltaV systems utilize username and password entry.</p> <p>Confirmer field is pre-populated with the username of the current DeltaV user.</p> <p>Confirmer can be changed to allow other users to take action at stations where they are not logged on.</p> <p>Verifier approval field is never pre-populated.</p> <p>Passwords are never displayed and are not accessible by any user.</p>	<p>DeltaV systems utilize username and password entry.</p> <p>Confirmer field is pre-populated with the username of the current DeltaV user.</p> <p>Confirmer can be changed to allow other users to take action at stations where they are not logged on.</p> <p>Verifier approval field is never pre-populated.</p> <p>Passwords are never displayed and are not accessible by any user.</p>	<p>DeltaV system uses username and password entry.</p> <p>Confirmer field is pre-populated with the username of the current DeltaV user.</p> <p>Confirmer can be changed to allow other users to take action at stations where they are not logged on.</p> <p>Verifier approval field is never pre-populated.</p> <p>Passwords are never displayed and are not accessible by any user.</p>

21CFR Sec. 11.200 Electronic Signature Components and Controls	Configuration Engineering Application	Run Time Application	History Application
<p>(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.</p> <p>(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.</p>	<p>If the user has logged off the system.</p>	<p>Confirm and verify signature feature (when enabled) may require sign off with user name and password for operator actions through DeltaV Operate, Control Studio online, the Batch Operator Interface and Campaign Manager Operator Interface.</p> <p>Confirmer field is pre-populated with the username of the current DeltaV user.</p> <p>Confirmer can be changed to allow other users to take action at stations where they are not logged on.</p> <p>Verifier approval field is never pre-populated.</p> <p>Passwords are never displayed and are not accessible by any user.</p>	<p>Not applicable</p>
<p>(2) Be used only by their genuine owners; and</p>	<p>DeltaV customers are responsible for ensuring that non-biometric electronic signatures are used only by their genuine owners</p>	<p>DeltaV customers are responsible for ensuring that non-biometric electronic signatures are used only by their genuine owners.</p>	<p>DeltaV customers are responsible for ensuring that non-biometric electronic signatures are used only by their genuine owners.</p>
<p>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.</p>	<p>DeltaV customers are responsible for ensuring compliance.</p>	<p>DeltaV customers are responsible for ensuring compliance.</p>	<p>DeltaV customers are responsible for ensuring compliance.</p>

21CFR Sec. 11.200 Electronic Signature Components and Controls	Configuration Engineering Application	Run Time Application	History Application
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than genuine owners.	Not applicable	Not applicable	Not applicable

21CFR Sec. 11.300 Controls for Identification Codes/ Passwords	Configuration Engineering Application	Run Time Application	History Application
<p>11.300</p> <p>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:</p>			
(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.	<p>DeltaV security layered on Windows security.</p> <p>Windows security policies allow for uniqueness of each user ID and password combination.</p> <p>Users may be locked out a users after a predefined number login failures.</p> <p>Security audit logs.</p> <p>Domain support is provided in the DeltaV system.</p>	<p>DeltaV security layered on Windows security.</p> <p>Windows policies allow for uniqueness of each user ID and password combination.</p> <p>Users may be locked out a users after a predefined number login failures.</p> <p>Security audit logs.</p> <p>Domain support is provided in the DeltaV system.</p>	<p>DeltaV security layered on Windows security.</p> <p>Windows policies allow for uniqueness of each user ID and password combination.</p> <p>Users may be locked out after a predefined number login failures.</p> <p>Security audit logs.</p> <p>Domain support is provided in DeltaV system.</p>

21CFR Sec. 11.300 Controls for Identification Codes/ Passwords	Configuration Engineering Application	Run Time Application	History Application
<p>(b) Ensuring that identification code and password issuances are periodically checked, recalled or revised (e.g. to cover such events as password aging).</p>	<p>DeltaV system security is based on Windows security, and can be configured to expire passwords on a periodic basis.</p> <p>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.</p>	<p>DeltaV system security is based on Windows security, and can be configured to expire passwords on a periodic basis.</p> <p>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.</p>	<p>DeltaV system security is based on Windows security, and can be configured to expire passwords on a periodic basis.</p> <p>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.</p>
<p>(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.</p>	<p>DeltaV customers are responsible for employing controls to ensure the security and integrity of identification codes and passwords.</p>	<p>DeltaV customers are responsible for employing controls to ensure the security and integrity of identification codes and passwords.</p>	<p>DeltaV customers are responsible for employing controls to ensure the security and integrity of identification codes and passwords.</p>

21CFR Sec. 11.300 Controls for Identification Codes/ Passwords	Configuration Engineering Application	Run Time Application	History Application
<p>(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.</p>	<p>DeltaV system security is based on Windows security, and can be configured to expire passwords on a periodic basis.</p> <p>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.</p>	<p>DeltaV system security is based on Windows security, and can be configured to expire passwords on a periodic basis.</p> <p>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.</p>	<p>DeltaV system security is based on Windows security, and can be configured to expire passwords on a periodic basis.</p> <p>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.</p>
<p>(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.</p>	<p>Customers are responsible for ensuring compliance.</p>	<p>Customers are responsible for ensuring compliance.</p>	<p>Customers are responsible for ensuring compliance.</p>

Appendix B – DeltaV Reference Table for Annex 11

Annex 11 Section #	Configuration Engineering Application	Run Time Application	History Application
1 - Risk Management	Not applicable	Not applicable	Not applicable
2 - Personnel	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.	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.
3 - Suppliers and Service Providers	Not applicable	Not applicable	Not applicable
4 - Validation	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.	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.	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.
4.1 - Life Cycle Management	Not applicable	Not applicable	Not applicable
4.2 - Change Controls	The DeltaV configuration 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). A rollback feature allows restoring to previous versions of a configuration item.	Not applicable	Not applicable
4.3 - Systems Inventory	Not applicable	Not applicable	Not applicable

Annex 11 Section #	Configuration Engineering Application	Run Time Application	History Application
4.4 - User Requirements Specifications	Not applicable	Not applicable	Not applicable
4.5 - Quality Management System	Not applicable	Not applicable	Not applicable
4.6 - Customized Systems	Not applicable	Not applicable	Not applicable
4.7 - Evidence of Appropriate Test Methods	Not applicable	Not applicable	Not applicable
4.8 - Data Transfer Validation	<p>Only DeltaV terminals can enter data and perform control actions.</p> <p>The system enforces validity checks since a device must be defined in the DeltaV Explorer and downloaded from the DeltaV engineering stations to become a valid device.</p>	<p>Only DeltaV terminals can enter data and perform control actions.</p> <p>The system enforces validity checks since a device must be defined in the DeltaV Explorer and downloaded from the DeltaV engineering stations to become a valid device.</p>	<p>Only DeltaV terminals can enter data and perform control actions.</p> <p>The system enforces validity checks since a device must be defined in the DeltaV Explorer and downloaded from the DeltaV engineering stations to become a valid device.</p>
<p>5 – Data</p> <p>6 – Accuracy Check</p>	<p>Audit Trail will capture modifications to the DeltaV configuration database, tracking who, where, when, and what.</p>	<p>Operator actions from DeltaV Operate, Control Studio online, the Batch Operator Interface and Campaign Manager Operator Interface can be configured to require confirmer and verifier authentication.</p> <p>Operator prompts can be configured to require confirmer and verifier authentication.</p> <p>Operator must have security key(s) for the area in which the action is being taken.</p> <p>Auto logout after extended period of inactivity.</p>	<p>Not applicable</p>

Annex 11 Section #	Configuration Engineering Application	Run Time Application	History Application
<p>7 – Data Storage 7.2 – Backup 17 - Archiving</p>	<p>Built-in security controls access to DeltaV configuration applications and database administration tools.</p> <p>Complete set of database administration tools that facilitate DB backup and restore are available.</p> <p>Configuration audit trail provides version tracking and supports item recovery and rollback.</p> <p>Customers should establish policies and procedures to ensure that records are retained for an appropriate duration of time.</p>	<p>Not applicable</p>	<p>Built-in security controls access to historical data.</p> <p>Data archival support for both continuous and batch data.</p> <p>Batch Historian administrator tool does not allow for the deletion of a batch history that has not been archived.</p> <p>Ability to “re-import” previously archived data.</p> <p>Customers should establish policies and procedures to ensure that records are retained for duration of an appropriate time.</p>

Annex 11 Section #	Configuration Engineering Application	Run Time Application	History Application
<p>7.1 – Secured and Accessible</p> <p>12 – Security</p> <p>12.1 - Physical/Logical</p>	<p>DeltaV built-in security system that is layered on Windows security.</p> <p>Uses the concept of locks and keys to assign system functions, field and parameters to authorized users.</p> <p>Access controlled by function & plant area.</p> <p>Configuration data files created with read-only access.</p> <p>Uses Microsoft Remote Desktop to provide remote login capability to DeltaV Terminal Server. Only specific workstations and users are authorized to establish remote desktop connection with the server. Once a remote session is established with a DeltaV Terminal Server, user will then have access to DeltaV functions based on his/her user privileges.</p>	<p>DeltaV built-in security system that is layered on Windows security.</p> <p>Uses the concept of locks and keys to assign system functions, field and parameters to authorized users.</p> <p>Access controlled by function & plant area.</p> <p>Operator confirmation and verifier approval options available in run time environment.</p> <p>Uses Microsoft Remote Desktop to provide remote login capability to DeltaV Terminal Server. Only specific workstations and users are authorized to establish remote desktop connection with the server. Once a remote session is established with a DeltaV Terminal Server, user will then have access to DeltaV functions based on his/her user privileges.</p>	<p>DeltaV built-in security system that is layered onto Windows security.</p> <p>Uses the concept of locks and keys to assign system functions, field and parameters to authorized users.</p> <p>Access controlled by function & plant area.</p> <p>Historical data files created with read-only access.</p> <p>DeltaV system provides authority checks to ensure that only authorized individuals can use the batch history and continuous historian applications.</p> <p>The DeltaV system provides no access to modify data by anyone with any level of security access.</p> <p>Batch history data may be deleted from the system only after they have been archived.</p>

Annex 11 Section #	Configuration Engineering Application	Run Time Application	History Application
	<p>DeltaV Virtualization supports the use of virtual machines and thin client workstations connected to the DeltaV Virtualization Networks. DeltaV Virtualization Networks must be isolated to prevent unauthorized access to the DeltaV virtual servers. DeltaV Remote Desktop Connection is the mechanism by which authorized users will connect to a DeltaV virtual machine using a thin client workstation.</p> <p>DeltaV system provides authority checks to ensure only authorized individuals can use the configuration engineering application. This is enabled via the DeltaV security system.</p>	<p>DeltaV Virtualization supports the use of virtual machines and thin client workstations connected to the DeltaV Virtualization Networks. DeltaV Virtualization Networks must be isolated to prevent unauthorized access to the DeltaV virtual servers. DeltaV Remote Desktop Connection is the mechanism by which authorized users will connect to a DeltaV virtual machine using a thin client workstation.</p> <p>DeltaV system provides authority checks to ensure that only authorized individuals can perform operator actions from DeltaV Operate, Control Studio online, the Batch Operator Interface and Campaign Manager Operator Interface.</p>	

Annex 11 Section #	Configuration Engineering Application	Run Time Application	History Application
8 - Printout	<p>Configuration applications (Explorer, Control Studio, Recipe Studio, etc.) allow viewing of all DeltaV configuration items.</p> <p>All configuration data may be printed from the configuration applications.</p> <p>Configuration audit trail information may also be viewed on-line and printed.</p>	Not applicable	<p>Batch data stored in SQL database - reports created using standard programming tools including Microsoft Visual Basic.</p> <p>Batch history view supports electronic viewing and printing of data.</p> <p>Continuous history is stored in a proprietary database. This information is available from the Process History View client. This can be displayed and printed.</p> <p>Applications to export data into other environments for analysis (e.g. Access, Excel).</p>

Annex 11 Section #	Configuration Engineering Application	Run Time Application	History Application
9 – Audit Trail 12.4 - Data Management / Operator Entries	<p>Configuration audit trail tracks who, where, when and what.</p> <p>Provides comprehensive version management and change tracking.</p> <p>Version to version “differences” can be viewed on line and printed.</p> <p>Provides the ability to rollback and restore previous versions of a configuration item.</p>	<p>All Operator actions are recorded in a secure time and date stamped electronic record. Both old and new values of the changed parameter are captured during a user change event from the controller (does not include changes to the Batch Execute and Historians). Within DeltaV, electronic records are not able to be modified or deleted.</p> <p>Time synchronization is provided for all devices in the system with time resynchronization after disaster recovery.</p> <p><i>Note: The logging of the old/previous value during a user change event is available in DeltaV v13.3.1 or later.</i></p>	<p>The Batch Historian is the secure data repository for long-term storage of the time and date stamped events generated by the Batch Executive.</p> <p>Batch Historian will collect the secure, time and date stamped history of all operator and alarms events.</p> <p>All historical files are write protected</p> <p>No provisions in the DeltaV system to change or delete historical records.</p> <p>Operator comments are linked to existing record.</p> <p>Audit trail of all actions taken through the Batch Historian interface.</p>
10 - Change and Configuration Management	DeltaV customers are responsible for developing policies and procedures to support the use of the applications in a regulated environment.	<i>DeltaV customers are responsible for developing policies and procedures to support the use of the applications in a regulated environment.</i>	DeltaV customers are responsible for developing policies and procedures to support the use of the applications in a regulated environment.
11 - Period Evaluation	DeltaV customers are responsible for period evaluation of their computerized systems.	DeltaV customers are responsible for period evaluation of their computerized systems.	DeltaV customers are responsible for period evaluation of their computerized systems.
12.2 - Critically	Not applicable	Not applicable	Not applicable

Annex 11 Section #	Configuration Engineering Application	Run Time Application	History Application
12.3 - Security Change Controls	<p>DeltaV system security is based on Windows security, and can be configured to expire passwords on a periodic basis.</p> <p>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.</p> <p>DeltaV customers are responsible for employing controls to ensure the security and integrity of identification codes and passwords.</p>	<p>DeltaV system security is based on Windows security, and can be configured to expire passwords on a periodic basis.</p> <p>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.</p> <p>DeltaV customers are responsible for employing controls to ensure the security and integrity of identification codes and passwords.</p>	<p>DeltaV system security is based on Windows security, and can be configured to expire passwords on a periodic basis.</p> <p>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.</p> <p>DeltaV customers are responsible for employing controls to ensure the security and integrity of identification codes and passwords.</p>
13 – Incident Management	Not applicable	Not applicable	Not applicable
14 - Electronic Signature	<p>Include name of signer (username) as well as complete name if available.</p> <p>Separate signatures and security keys for “confirmers” and “verifiers.”</p>	<p>Include name of signer (username) as well as complete name if available.</p> <p>All event and historical data records include date and time stamps.</p> <p>Separate signatures and security keys for “confirmers” and “verifiers.”</p>	<p>Include name of signer (username) as well as complete name if available.</p> <p>All historical data records include date and time stamps.</p> <p>Separate signatures and security keys for “confirmers” and “verifiers.”</p>

Annex 11 Section #	Configuration Engineering Application	Run Time Application	History Application
14 (a) - Same as Hand-written	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.	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.
14 (b) - Permanent Link	Electronic signatures are integral part of batch history and event log. 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 and event log. 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 and event log. DeltaV Data View and Analysis tools do not provide any mechanism to allow the modification or deletion of a record.
14 (c) - Time and Date	Configuration audit trail tracks who, where, when and what.	All Operator actions are recorded in a secure time and date stamped electronic record.	Batch Historian will collect the secure, time and date stamped history of all operator and alarms events.
15 – Batch Release	DeltaV customers are responsible for making sure that only qualified persons are to certify the release of the batches.	DeltaV customers are responsible for making sure that only qualified persons are to certify the release of the batches.	DeltaV customers are responsible for making sure that only qualified persons are to certify the release of the batches.
16 - Business Continuity	Not applicable	Not applicable	Not applicable

Appendix C – DeltaV Reference Table for MHRA Data Integrity Definitions and Guidance

Term	Expectation / Guidance	DeltaV Reference
Data / Data Integrity	<p>Data integrity arrangements must ensure that the accuracy, completeness, content and meaning of data is retained throughout the data lifecycle.</p> <p>Complete, consistent, and accurate data should be:</p> <ul style="list-style-type: none"> ■ A - attributable to the person generating the data ■ L – legible and permanent ■ C – contemporaneous ■ O - original record (or ‘true copy’) ■ A - accurate 	<p>A – attributable to the person generating the data.</p> <ul style="list-style-type: none"> ■ Engineering revisions and changes can be tracked as changes are made using the DeltaV Configuration Audit Trail application. 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. ■ All operator actions are recorded in a secure time- and date-stamped electronic record. Both old and new values of the changed parameter are captured during a user change event. ■ Batch-related events are captured as an electronic record in the Batch Historian and include a time and date stamp, the identity of the person making the entry, and the location from which the change was made. <p>L – legible and permanent.</p> <ul style="list-style-type: none"> ■ All configuration and historical data files are stored in secured data repository with write-access given only to the applications that need to write data to those files. ■ Historical data may be deleted from the system only after they have been archived. This ensures data are stored permanently and protect against accidental deletion of data. ■ 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 native DeltaV file and database formats, or can be exported in different file formats including text, Microsoft Word and Microsoft Excel for viewing and reporting purpose.

Term	Expectation / Guidance	DeltaV Reference
		<p>C – contemporaneous.</p> <ul style="list-style-type: none"> ■ All configuration and operator actions are recorded at the time the work is performed with a time and date stamp, the identity of the person making the entry, and the location from which the change was made. <p>O – original record or true copy.</p> <ul style="list-style-type: none"> ■ The validity of the source of DeltaV data input is restricted to DeltaV devices only. All DeltaV workstations, controllers, and I/O devices must be defined in the DeltaV Explorer and downloaded before they can generate, enter, record and process data in DeltaV. Devices connected to the DeltaV that are not configured in the DeltaV Explorer are not recognized by the DeltaV system and are not allowed to participate in DeltaV communication. ■ All configuration, operation and historical data files are stored in its original format in secured data repository. Historical data can only be deleted from the system after they have been archived to ensure a true copy of the original data is maintained securely throughout the records retention period. <p>A – accurate.</p> <ul style="list-style-type: none"> ■ Built-in security controls access to configuration, operation and historical data to protect against data falsification accidental modification. ■ Comprehensive version management and change tracking, including the ability to log all operator actions with old and new values of the changed parameter ensure all data changes are recorded and data accuracy and consistency is maintained throughout the data lifecycle.

Term	Expectation / Guidance	DeltaV Reference
Data governance	<p>Data governance should address data ownership throughout the lifecycle, and consider the design, operation and monitoring of processes / systems in order to comply with the principles of data integrity including control over intentional and unintentional changes to information.</p>	<p>All DeltaV data sources including workstations, controllers, and I/O devices must be defined in the DeltaV Explorer and downloaded before they can participate generate, enter, record and process data in DeltaV.</p> <p>DeltaV data are stored in its original format in secured data repository to ensure that all data are complete and available.</p> <p>Historical data can only be deleted from the system after they have been archived to ensure a true copy of the original data is maintained securely throughout the records retention period.</p> <p>DeltaV systems provide built-in security to control access to configuration, operation and historical data to protect against data falsification and accidental modification. Comprehensive version management and change tracking, including the ability to log all operator actions with old and new values of the changed parameter ensure all data changes are recorded.</p> <p>The DeltaV data security system and audit trail capabilities ensure that data accuracy and consistency is maintained throughout the data lifecycle.</p>
Data Lifecycle	<p>The procedures for destruction of data should consider data criticality and legislative retention requirements. Archival arrangements should be in place for long term retention (in some cases, periods up to 30 years) for records such as batch documents, marketing authorisation application data, traceability data for human-derived starting materials (not an exhaustive list). Additionally, at least 2 years of data must be retrievable in a timely manner for the purposes of regulatory inspection.</p>	<p>The DeltaV system has built-in security that controls access to DeltaV configuration applications and database administration tools.</p> <p>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.</p> <p>The Batch Historian Administrator application does not allow for the deletion of a batch history that has not been archived.</p>

Term	Expectation / Guidance	DeltaV Reference
Primary Record	<p>In situations where the same information is recorded concurrently by more than one system, the data owner should define which system generates and retains the primary record, in case of discrepancy. The 'primary record' attribute should be defined in the quality system, and should not be changed on a case by case basis.</p> <p>Risk management principles should be used to ensure that the assigned 'primary record' provides the greatest accuracy, completeness, content and meaning. For instance, it is not appropriate for low-resolution or static (printed / manual) data to be designated as a primary record in preference to high resolution or dynamic (electronic) data. All data should be considered when performing a risk based investigation into data anomalies (e.g. out of specification results).</p>	Not applicable

Term	Expectation / Guidance	DeltaV Reference
Original record / True Copy:	<p>Original records and true copies must preserve the integrity (accuracy, completeness, content and meaning) of the record. Exact (true) copies of original records may be retained in place of the original record (e.g. scan of a paper record), provided that a documented system is in place to verify and record the integrity of the copy.</p> <p>It is conceivable for raw data generated by electronic means to be retained in an acceptable paper or pdf format, where it can be justified that a static record maintains the integrity of the original data. However, the data retention process must be shown to include verified copies of all raw data, metadata, relevant audit trail and result files, software / system configuration settings specific to each analytical run *, and all data processing runs (including methods and audit trails) necessary for reconstruction of a given raw data set. It would also require a documented means to verify that the printed records were an accurate representation. This approach is likely to be onerous in its administration to enable a GMP compliant record.</p> <p>Many electronic records are important to retain in their dynamic (electronic) format, to enable interaction with the data. Data must be retained in a dynamic form where this is critical to its integrity or later verification. This should be justified based on risk.</p> <p>* computerised system configuration settings should be defined, tested, 'locked' and protected from unauthorised access as part of computer system validation. Only those variable settings which relate to an analytical run would be considered as electronic raw data.</p>	Refers to the "Data" section above.

Term	Expectation / Guidance	DeltaV Reference
Computer system transactions:	<p>Computer systems should be designed to ensure that the execution of critical operations are recorded contemporaneously by the user and are not combined into a single computer system transaction with other operations. A critical processing step is a parameter that must be within an appropriate limit, range, or distribution to ensure the desired product quality. These should be reflected in the process control strategy.</p> <p>Examples of 'units of work':</p> <ul style="list-style-type: none"> ■ Weighing of individual materials ■ Entry of process critical manufacturing / analytical parameters ■ Verification of the identity of each component or material that will be used in a batch ■ Verification of the addition of each individual raw material to a batch (e.g. when the sequence of addition is considered critical to process control – see figure 2) ■ Addition of multiple pre-weighed raw materials to bulk vessel when required as a single manufacturing step (e.g. when the sequence of addition is not considered critical to process control – see figure 3) 	<p>Operator actions from DeltaV Operate, Control Studio online, Batch Operator Interface and Campaign Manager Operator Interface can be configured to require Confirm and Verify authentication to ensure that the execution of critical operations are recorded contemporaneously.</p> <p>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.</p> <p>The confirmer and verifier must have the correct security key(s) for the area in which the action is being taken.</p>

Term	Expectation / Guidance	DeltaV Reference
Audit Trail	<p>Where computerised systems are used to capture, process, report or store raw data electronically, system design should always provide for the retention of full audit trails to show all changes to the data while retaining previous and original data. It should be possible to associate all changes to data with the persons making those changes, and changes should be time stamped and a reason given. Users should not have the ability to amend or switch off the audit trail.</p> <p>The relevance of data retained in audit trails should be considered by the company to permit robust data review / verification. The items included in audit trail should be those of relevance to permit reconstruction of the process or activity. It is not necessary for audit trail review to include every system activity (e.g. user log on/off, keystrokes etc.), and may be achieved by review of designed and validated system reports.</p> <p>Audit trail review should be part of the routine data review / approval process, usually performed by the operational area which has generated the data (e.g. laboratory). There should be evidence available to confirm that review of the relevant audit trails have taken place. When designing a system for review of audit trails, this may be limited to those with GMP relevance (e.g. relating to data creation, processing, modification and deletion etc). Audit trails may be reviewed as a list of relevant data, or by a validated 'exception reporting' process. QA should also review a sample of relevant audit trails, raw data and metadata as part of self inspection to ensure on-going compliance with the data governance policy / procedures.</p>	<p>The DeltaV system provides audit trails functionalities in the Configuration, Run Time, and History environments:</p> <p>Configuration Application</p> <p>Engineering revisions and changes can be tracked as changes are made using the DeltaV Configuration Audit Trail application. This application creates and maintains a complete 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.</p> <p>Run Time Application</p> <p>All operator actions are recorded in a secure time- and date-stamped electronic record. Both old and new values of the changed parameter are captured during a user change event.</p> <p>History Application</p> <p>Batch-related events are captured as an electronic record in the Batch Historian and include a time and date stamp, the identity of the person making the entry, and the location from which the change was made.</p>

Term	Expectation / Guidance	DeltaV Reference
Data Review	<p>There should be a procedure which describes the process for the review and approval of data, including raw data. Data review must also include a review of relevant metadata, including audit trail.</p> <p>Data review must be documented.</p> <p>A procedure should describe the actions to be taken if data review identifies an error or omission. This procedure should enable data corrections or clarifications to be made in a GMP compliant manner, providing visibility of the original record, and audit trailed traceability of the correction, using ALCOA principles (see 'data' definition).</p>	DeltaV customers are responsible for developing policies and procedures for review and approval of data.

Term	Expectation / Guidance	DeltaV Reference
<p>Computerised system user access / system administrator roles</p>	<p>Full use should be made of access controls to ensure that people have access only to functionality that is appropriate for their job role, and that actions are attributable to a specific individual. Companies must be able to demonstrate the access levels granted to individual staff members and ensure that historical information regarding user access level is available.</p> <p>Shared logins or generic user access should not be used. Where the computerised system design supports individual user access, this function must be used. This may require the purchase of additional licences.</p> <p>It is acknowledged that some computerised systems support only a single user login or limited numbers of user logins. Where alternative computerised systems have the ability to provide the required number of unique logins, facilities should upgrade to an appropriate system by the end of 2017. Where no suitable alternative computerised system is available, a paper based method of providing traceability will be permitted. The lack of suitability of alternative systems should be justified based on a review of system design, and documented.</p> <p>System administrator access should be restricted to the minimum number of people possible taking account of the size and nature of the organisation. The generic system administrator account should not be available for use. Personnel with system administrator access should log in under unique log-ins that allow actions in the audit trail(s) to be attributed to a specific individual.</p>	<p>The DeltaV system provides authority checks to ensure only authorized individuals can access to DeltaV configuration applications, database administration tools, and runtime operations. The security system is layered on the Windows security system and 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.</p> <p>Configuration and Historical data files are created with read-only access.</p> <p>Operator confirmation and verifier approval options available in run time environment.</p> <p>The DeltaV system uses Microsoft Remote Desktop to provide remote login capability to DeltaV Terminal Server in both the traditional DeltaV architecture and Virtualization environment. Only authorized workstations and users are allowed to establish remote desktop connection with the server. This prevents unauthorized users or workstations to connect remotely. Once a remote session is permitted with a DeltaV Terminal Server, the user will then have access to the system through the DeltaV FlexLock and built-in security system based on his/her user privileges.</p> <p>The use of shared login accounts is strongly discouraged in DeltaV systems, as many operations (configuration and runtime) are logged, sharing accounts makes it difficult to identify the individual that performed an operation by reviewing the DeltaV event and historical log.</p> <p>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 general approach is to give administrative privileges 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.</p>

Term	Expectation / Guidance	DeltaV Reference
	<p>System Administrator rights (permitting activities such as data deletion, database amendment or system configuration changes) should not be assigned to individuals with a direct interest in the data (data generation, data review or approval). Where this is unavoidable in the organisational structure, a similar level of control may be achieved by the use of dual user accounts with different privileges. All changes performed under system administrator access must be visible to, and approved within, the quality system.</p> <p>The individual should log in using the account with the appropriate access rights for the given task e.g. a laboratory manager performing data checking should not log in as system administrator where a more appropriate level of access exists for that task.</p>	
Data retention	<p>Raw data (or a true copy thereof) generated in paper format may be retained for example by scanning, provided that there is a process in place to ensure that the copy is verified to ensure its completeness.</p> <p>Data retention may be classified as archive or backup</p> <p>Data and document retention arrangements should ensure the protection of records from deliberate or inadvertent alteration or loss.</p> <p>Secure controls must be in place to ensure the data Integrity of the record throughout the retention period, and validated where appropriate.</p> <p>Where data and document retention is contracted to a third party, particular attention should be paid to understanding the ownership and retrieval of data held under this arrangement. The physical location in which the data is held, including impact of any laws applicable to that geographic location should also be considered. The responsibilities of the contract giver and acceptor must be defined in a contract as described in Chapter 7 of the GMP Guide</p>	<p>Built-in security controls access to DeltaV configuration applications and database administration tools to prevent deliberate or inadvertent data alteration or loss.</p> <p>Data archival support for both continuous and batch data.</p> <p>Complete set of database administration tools that facilitate DB backup and restore are available.</p> <p>Configuration audit trail provides version tracking and supports item recovery and rollback.</p> <p>Batch Historian administrator tool does not allow for the deletion of a batch history that has not been archived.</p> <p>Customers should establish policies and procedures to ensure that records are retained for an appropriate duration of time.</p>

Term	Expectation / Guidance	DeltaV Reference
File structure - Flat files	<p>File structure has a significant impact on the inherent data integrity risks. The ability to manipulate or delete flat files requires a higher level of logical and procedural control over data generation, review and storage.</p> <p>Flat files may carry basic metadata relating to file creation and date of last amendment, but may not audit trail the type and sequence of amendments. When creating flat file reports from electronic data, the metadata and audit trails relating to the generation of the raw data may be lost, unless these are retained as a 'true copy'.</p> <p>Consideration also needs to be given to the 'dynamic' nature of the data, where appropriate (see 'true copy' definition)</p> <p>There is an inherently greater data integrity risk with flat files (e.g. when compared to data contained within a relational database), in that these are easier to manipulate and delete as a single file.</p>	DeltaV configuration files are created with read-only access with built-in security to control access to DeltaV configuration applications.
File structure - Relational Database	<p>This file structure is inherently more secure, as the data is held in a large file format which preserves the relationship between data and metadata. This is more resilient to attempts to selectively delete, amend or recreate data and the metadata trail of actions, compared to a flat file system.</p> <p>Retrieval of information from a relational database requires a database search tool, or the original application which created the record.</p>	The DeltaV Event Chronicle and Historian are stored in relational database with built-in security to control access to DeltaV database administration tools.

Term	Expectation / Guidance	DeltaV Reference
Validation - for intended purpose	<p>Computerised systems should comply with the requirements of EU GMP Annex 11 and be validated for their intended purpose. This requires an understanding of the computerised system’s function within a process. For this reason, the acceptance of vendor-supplied validation data in isolation of system configuration and intended use is not acceptable. In isolation from the intended process or end user IT infrastructure, vendor testing is likely to be limited to functional verification only, and may not fulfil the requirements for performance qualification.</p> <p>For example - validation of computerised system audit trail</p> <ul style="list-style-type: none"> ■ A custom report generated from a relational database may be used as a GMP system audit trail. ■ SOPs should be drafted during OQ to describe the process for audit trail verification, including definition of the data to be reviewed. ■ ‘Validation for intended use’ would include testing during PQ to confirm that the required data is correctly extracted by the custom report, and presented in a manner which is aligned with the data review process described in the SOP. 	<p>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.</p>

Emerson
North America, Latin America:
 ☎ +1 800 833 8314 or
 ☎ +1 512 832 3774

Asia Pacific:
 ☎ +65 6777 8211

Europe, Middle East:
 ☎ +41 41 768 6111

🌐 www.emerson.com/deltav

©2017, Emerson. All rights reserved.

The Emerson logo is a trademark and service mark of Emerson Electric Co. The DeltaV logo is a mark of one of the Emerson family of companies. All other marks are the property of their respective owners.

The contents of this publication are presented for informational purposes only, and while every effort has been made to ensure their accuracy, they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. All sales are governed by our terms and conditions, which are available on request. We reserve the right to modify or improve the designs or specifications of our products at any time without notice.