FactoryTalk® View Machine Edition 10.00

Complying with 21 CFR Part 11: Electronic Records & Signatures
## Table of Contents

Introduction .................................................................................................................................................. 3
Defining Key Terms ...................................................................................................................................... 4
FactoryTalk® View ME and PanelView™ Plus 6/7 in a Control System ......................................................... 5
  PanelView Plus 6/7 .................................................................................................................................... 5
  FactoryTalk View ME ................................................................................................................................. 5
  How FactoryTalk Services Platform Fits In ............................................................................................... 5
  How FactoryTalk AssetCentre Fits In ......................................................................................................... 5
  How FactoryTalk ViewPoint Fits In .......................................................................................................... 5
Complying with the Part 11 Regulation ......................................................................................................... 6
  21 CFR Part 11 Compliance Qualitative Summary .................................................................................... 6
  Table 1: Subpart B – Electronic Records .................................................................................................. 7
  Table 2: Subpart C – Electronic Signatures ............................................................................................. 10
  Limit Physical Access to Computer Hardware .......................................................................................... 14
  Take Advantage of Microsoft Windows Active Directory ...................................................................... 14
  Configure the System to Use Windows-linked User Accounts ................................................................ 14
    Use Windows Account Password Aging and Management ........................................................................ 15
    Managing Windows-linked Security Configuration in a Running Application ........................................... 15
    Configure Windows Active Directory Authentication on the PanelView Plus 6/7 Terminal ....................... 15
  Configure the System to Use FactoryTalk Security User Accounts ......................................................... 16
    Use FactoryTalk Security Account Password Aging and Management ..................................................... 16
    Managing Native FactoryTalk Users and Groups in a Running Application .......................................... 17
Application Design to Enable 21 CFR Part 11 Compliance .......................................................................... 17
  Configure FactoryTalk View Runtime Security Codes for Security Accounts ............................................ 18
  Configure System Operator Inactivity Action ............................................................................................. 18
  Require Operators to Log In to Use the System ....................................................................................... 18
  Require Re-verification of Operator Identity, or Supervisor Signoff ......................................................... 19
  Logging Operator Activity ......................................................................................................................... 20
  Detecting Local Onboard Audit and Alarm Circular Buffer Capacity Conditions .................................... 22
  Exporting Local Onboard Application Audit and Alarm Information ..................................................... 23
  Clearing the Audit or Alarm History Buffers ............................................................................................. 24
  Capturing Process Data ............................................................................................................................. 25
  Detecting Changes in Exported CSV Files ............................................................................................... 26
  Limit Access to Configuration Mode and Shutdown Buttons .................................................................... 26
  Supporting Remote Access to the Application ........................................................................................... 26
Control Microsoft Windows CE Desktop Access on PanelView Plus 6/7 Terminal ...................................... 28
  Use of the PanelView Plus 6/7 Password-enabled Screensaver ................................................................... 29
  Use Version Control Software.................................................................................................................... 29
About Rockwell Automation ......................................................................................................................... 30
  Publishing Application Notes .................................................................................................................... 30
  References .................................................................................................................................................. 30
Appendix A – FactoryTalk View Machine Edition Objects Supporting Electronic Signature .................... 31
Introduction

In 1997 the Food and Drug Administration (FDA) issued the final rule on the criteria under which the Agency will accept electronic signatures and records in place of handwritten signatures and records executed on paper. The scope of this regulation, US FDA 21 CFR Part 11, is significant and impacts all computer systems related to the manufacturing of a life science product (for example, oral solid dosage, biologic, or medical device). According to the rule, “This Part (21 CFR Part 11) applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted.” Legacy systems, including Microsoft Access database software and Microsoft Excel spreadsheet software, are not protected by a legacy system clause. The dollar cost of remediating these systems calculates to a cost in the millions. However, the cost of not taking advantage of electronic records and signatures can be detrimental to the competitiveness of a company’s position in its marketplace.

The purpose of this document is to provide life science manufacturers with a description of how a FactoryTalk View Machine Edition (ME) v10.00 application, running on a PanelView™ Plus 6/7, MobileView™, or industrial computer, can address the technical requirements of Part 11. Each manufacturer has a set of unique needs and interpretation of Part 11; Rockwell Automation® recognizes the demands of life sciences manufacturers and has created a solution that is flexible enough to address these differences. The objective is to help life sciences manufacturers quickly and cost-effectively comply with 21 CFR Part 11.

FactoryTalk View ME 10.00 adds functionality designed for applications that must comply with 21 CFR Part 11. These enhancements were explicitly made to overcome compliance obstacles that exist in earlier versions of FactoryTalk View ME.

Onboard Audit

The new onboard audit feature records and stores operator’s actions locally. Locally storing the audit log allows the system to overcome the challenges of complying with 21 CFR Part 11 using FactoryTalk® AssetCentre as the FactoryTalk View ME audit log repository.

Export Logs to CSV

The system can export the audit history, alarm history, and diagnostic log to a CSV file. This information can be used to generate an electronic batch record.

Audit and Alarm History Capacity Triggers

Since the audit and alarm history are circular buffers, each with a 10,000 record maximum size, v10.00 introduces capacity triggers. The capacity triggers can be used to signal to the system or operator when the circular buffers reach a setpoint (percentage based). For example, the High Capacity trigger can be used to trigger an alarm when it is reached.
Defining Key Terms

Within the regulation are seven key terms that the FDA has defined:

**Closed System** – An environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system. This document assumes that a closed system is used.

**Open System** – An environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

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

**Biometrics** – A method of verifying an individual’s identity based on measurement of the individual’s physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

**Electronic Signature** – A computer data compilation of any symbol or series of symbols, executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual’s handwritten signature.

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

**Handwritten Signature** – The scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument, such as a pen or stylus, is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.
FactoryTalk View ME and PanelView Plus 6/7 in a Control System

PanelView Plus 6/7 is an electronic operator device. FactoryTalk View ME runs the user-designed application with which operators interact.

PanelView Plus 6/7
PanelView Plus 6 and PanelView Plus 7 terminals run Microsoft Windows CE 6.0 embedded operating system. The terminal hosts application software like FactoryTalk View ME. The system offers features to secure the Windows CE desktop.

FactoryTalk View ME
FactoryTalk View ME runs an application created by an HMI designer on a PanelView Plus 6, PanelView Plus 7, MobileView, or industrial computer. FactoryTalk View ME provides features that application designers can incorporate to create applications that can be deployed in environments that require 21 CFR Part 11 compliance. These features include user account management, operator audit trail, data logging, and electronic signature.

This document intends to describe how to use FactoryTalk View ME to secure and log operator actions, track alarms, and log other operational data.

How FactoryTalk Services Platform Fits In
FactoryTalk View ME uses the FactoryTalk Services Platform (FTSP), a set of software components and services that are shared by many Rockwell Automation® software products. FTSP provides FactoryTalk® software product with FactoryTalk® Diagnostics, which offers a consistent, reliable means for Rockwell Software® products to communicate and pass messages back and forth. This communication allows for the logging of event and audit messages from a PanelView Plus 6/7 executing a FactoryTalk® View ME HMI application to a centralized, common data store.

FTSP provides a security architecture that provides for local FactoryTalk® and Windows-linked user and groups. The HMI designer can implement and configure the security rights of these users and groups to control operator access.

How FactoryTalk AssetCentre Fits In
FactoryTalk AssetCentre is a set of tools designed to securely and centrally manage factory and process automation production environments by securing access to the control system, tracking users’ actions, managing asset configuration files, providing backup and recovery of operating asset configurations, and providing tools for the configuration of process instruments. The combination of this functionality allows for records of alterations to electronic files and the control and recording of user actions, as required by regulations such as 21 CFR Part 11.

How FactoryTalk ViewPoint Fits In
FactoryTalk ViewPoint provides a remote web browser-based connection to the FactoryTalk View ME application executing on a PanelView Plus 6/7. The HMI designer decides which displays are available from FactoryTalk ViewPoint. FactoryTalk ViewPoint maintains a security system that is separate from the runtime security in FactoryTalk View ME, thus runtime security changes made in FactoryTalk View ME are not reflected in FactoryTalk ViewPoint. When using local FactoryTalk® Security users and groups with FactoryTalk ViewPoint, it will be difficult to validate the system to 21 CFR Part 11. This situation can be mitigated by using Windows-linked groups since membership is managed in the Windows domain.

For most applications that must comply with 21 CFR Part 11 it is recommended that data changes via FactoryTalk ViewPoint are disabled.
Complying with the Part 11 Regulation

21 CFR Part 11 is composed of two major subparts (electronic records and electronic signatures) that provide guidelines that regulated companies must minimally follow to achieve the level of integrity, reliability, and consistency of electronic records and signatures acceptable to the FDA. Complying with the Part 11 regulation requires a combination of strong management procedures and computer systems that meet the technical aspect of the guideline such as application security, audit trails, and password protection. Rockwell Automation works with the life science industry to confirm that products like PanelView Plus 6/7 running FactoryTalk View ME v10.00 include features that are capable of satisfying the technical requirements of 21 CFR Part 11. As such, FactoryTalk View ME is flexible and configurable to meet the various SOPs and implementations needed to facilitate compliance with this regulation. However, each customer’s security and standard operating procedures (SOP) for supporting this regulation are unique.

The Qualitative Summary provides a high-level summary of how well FactoryTalk View ME meets the intent of the 21 CFR Part 11 regulation. The regulation requirements have been grouped by their functional intent to allow for easy understanding. Tables 1 and 2 provide more detailed information regarding the general functionality of FactoryTalk View ME relative to 21 CFR Part 11 compliance.

21 CFR Part 11 Compliance Qualitative Summary

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
<th>FactoryTalk View ME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Integrity</td>
<td>When PanelView Plus 6/7, running FactoryTalk View ME 10.00, is exporting audit log information to a CSV log file that is stored on removable media, if that media is unavailable or full, the audit log information will not be exported. It is incumbent on the end user to create a process to manage the audit logs on the terminals. The CSV log file does contain hash information, which makes it possible to detect any changes to the recorded information. When configured to forward audit log information to FactoryTalk AssetCentre, for FactoryTalk View ME 10.00 and earlier releases, there is no buffering or caching of audit messages in the local system. If the network connection to the FactoryTalk AssetCentre system is lost, operator audit information sent while the systems are disconnected will be lost.</td>
<td>(8.20) (9.00) (10.00)</td>
</tr>
<tr>
<td>Audit Trail, Change Control Support</td>
<td>FactoryTalk View ME records audit log information as operator actions occur. All tag writes are audited. System actions, such as a user logging in to acknowledge an alarm, are also audited. Data Integrity functional intent should be considered when evaluating any solution.</td>
<td>(8.20) (9.00) (10.00)</td>
</tr>
<tr>
<td>System Access, Identification Codes, and Passwords</td>
<td>FactoryTalk View ME uses FactoryTalk Security as the user authentication service. FactoryTalk Security can be integrated with a Microsoft Active Directory to provide centralized user management. When integrating with Microsoft Active Directory, ex. Windows Server 2008/2012/2016 Active Directory authentication is limited to LDAP or LDAP over SSL.</td>
<td>(8.20) (9.00) (10.00)</td>
</tr>
</tbody>
</table>
### Electronic Signatures

FactoryTalk View ME supports electronic signature. FactoryTalk View ME objects that write data can be configured to require an electronic signature. The HMI Designer must enable electronic signature for FactoryTalk View ME display objects as required by the application. The system will not otherwise require an electronic signature to write information to a tag.

### Open Systems

PanelView Plus 6/7 are closed systems.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Signatures</td>
<td>FactoryTalk View ME supports electronic signature. FactoryTalk View ME objects that write data can be configured to require an electronic signature. The HMI Designer must enable electronic signature for FactoryTalk View ME display objects as required by the application. The system will not otherwise require an electronic signature to write information to a tag.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FactoryTalk View ME</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.20</td>
</tr>
<tr>
<td>9.00</td>
</tr>
<tr>
<td>10.00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open Systems</td>
<td>PanelView Plus 6/7 are closed systems.</td>
</tr>
</tbody>
</table>

| Key: ● – Meets ● – Complies with considerations ○ – Does not meet |
|-----------------|------------------|

**Table 1: Subpart B – Electronic Records**

<table>
<thead>
<tr>
<th>Section</th>
<th>Requirements</th>
<th>FactoryTalk View ME 10.00 meets?</th>
<th>Application notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>§11.10</td>
<td>Controls for Closed Systems</td>
<td></td>
<td>System validation is unique in every case and must be done by the customer. Upon request, Rockwell Automation can assist with system validation.</td>
</tr>
<tr>
<td>a) Validation of systems to assist with accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</td>
<td>Yes No N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.</td>
<td>Yes No N/A</td>
<td>Audit records</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>FactoryTalk View ME generates an audit trail for operator actions. When using onboard auditing in v10.00, audits are persisted on the PanelView Plus 6/7 in a circular buffer with a maximum of 10,000 records. The records can be viewed within the application. The system provides flags that can be used to generate alarms when the circular buffer reaches a configurable High and High-high capacity, or overruns. The onboard audit cache can be exported to a CSV file. The export file contains information to allow for tamper detection using a tamper detection utility. When used with FactoryTalk AssetCentre, audits are sent to the FactoryTalk AssetCentre Audit database. All FactoryTalk AssetCentre records are stored in a SQL-compliant ODBC database that can be accessed with reporting tools. It is not possible to view or access FactoryTalk AssetCentre audits from FactoryTalk View ME. There is no buffering or caching of audit messages in the local system. If the network connection to the FactoryTalk AssetCentre system is lost, audits sent while the systems are disconnected will be lost. FactoryTalk View ME running on a PC (FactoryTalk View ME Station) cannot send messages to FactoryTalk AssetCentre.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Alarm records</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Alarms are always stored locally in a circular buffer with a maximum of 10,000 records. In v10.00, the system provides flags that can be used to generate alarms when the alarm circular buffer reaches a configurable High and High-high capacity, or overruns. The alarm cache can be exported to CSV file. The export file contains information to allow for tamper detection using a tamper detection utility.</td>
<td></td>
</tr>
<tr>
<td>Section</td>
<td>Requirements</td>
<td>FactoryTalk View ME 10.00 meets?</td>
<td>Application notes</td>
</tr>
<tr>
<td>---------</td>
<td>--------------</td>
<td>---------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>c)</td>
<td>Protection of records to enable their accurate and ready retrieval throughout the records retention period.</td>
<td>Yes ☑️ No ❑ N/A</td>
<td>Onboard records are stored in a proprietary file. A maximum of 10,000 records can be stored in the circular buffer. The system provides flags for configurable High and High-high buffer capacity, and an overrun flag. The flags can be tied to the intrinsic Alarm subsystem. The onboard audit cache can be exported to a CSV file. The export file contains information to allow for tamper detection using a tamper detection utility. FactoryTalk AssetCentre records are stored in an SQL-compliant ODBC database using FactoryTalk AssetCentre, and are available for viewing, printing, and exporting throughout the records retention period. There is no buffering or caching of audit messages in the local system. If the network connection to the FactoryTalk AssetCentre system is lost, operator audit information sent while the systems are disconnected will be lost. FactoryTalk View ME running on a PC cannot send messages to FactoryTalk AssetCentre. Precautionary measures such as periodic backup of the database, or exporting the onboard audit to CSV, are procedures that customers should incorporate into their SOP.</td>
</tr>
<tr>
<td>d)</td>
<td>Limiting system access to authorized individuals.</td>
<td>Yes ☑️ No ❑ N/A</td>
<td>Limiting system access includes configuring FactoryTalk View ME to use FactoryTalk Security or Windows-linked users/groups. It also includes using other security measures, such as FactoryTalk View ME Runtime security to set operator access, and restricting PanelView Plus 6/7 Desktop Access, which helps prevent unauthorized access to data files and the operating system.</td>
</tr>
<tr>
<td>e)</td>
<td>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.</td>
<td>Yes ☑️ No ❑ N/A</td>
<td>User activity is logged to either an onboard circular buffer or FactoryTalk AssetCentre. The log identifies the time and date the action occurred and the name of the logged-in operator who performed the action, and the type of operation that was performed and the values of the changed item before and after the change. The customer’s SOP should include the retention period of the audit trail records.</td>
</tr>
<tr>
<td>f)</td>
<td>Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.</td>
<td>Yes ☑️ No ❑ N/A</td>
<td>Operational steps and sequencing are implemented as a combination of controller logic and FactoryTalk View ME. FactoryTalk View ME supports screen-level security. An application can be developed to support user-initiated operational checks, which require screen security and electronic signatures.</td>
</tr>
<tr>
<td>g)</td>
<td>Use of authority checks to help provide confidence 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.</td>
<td>Yes ☑️ No ❑ N/A</td>
<td>FactoryTalk View ME uses a combination of native FactoryTalk Security, Microsoft Windows domain security, and FactoryTalk View ME runtime security. Customers should implement policies and administrative procedures to define authorized access to the system. Many graphic objects available in FactoryTalk View ME v8.20 and later can be configured to require an electronic signature. The electronic signature can be configured to require the operator to reauthenticate, or both the operator and a member of a pre-configured approver group to reauthenticate, to complete the electronic signature. The list of electronic signature capable objects can be found in Appendix A.</td>
</tr>
<tr>
<td>Section</td>
<td>Requirements</td>
<td>FactoryTalk View ME 10.00 meets?</td>
<td>Application notes</td>
</tr>
<tr>
<td>---------</td>
<td>--------------</td>
<td>---------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>h)</td>
<td>Use of device (for example, terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.</td>
<td><img src="#" alt="Yes" /> <img src="#" alt="No" /> <img src="#" alt="N/A" /></td>
<td>FactoryTalk View ME uses functions such as operator login and electronic signature to validate the source of data input. FactoryTalk View ME numeric entry controls provide minimum and maximum limits for data entry. It is incumbent on the HMI Designer to confirm they are included and appropriately configured in an HMI application. Many graphic objects available in FactoryTalk View ME v8.20 and later can be configured to require an electronic signature. The electronic signature can be configured to require the operator to reauthenticate, or both the operator and a member of a pre-configured approver group to reauthenticate, to complete the electronic signature. The list of electronic signature-capable objects can be found in Appendix A.</td>
</tr>
<tr>
<td>i)</td>
<td>Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.</td>
<td><img src="#" alt="Yes" /> <img src="#" alt="No" /> <img src="#" alt="N/A" /></td>
<td>Customers are responsible for hiring and training appropriate staff members with the education, training, and experience to perform assigned tasks. FactoryTalk View ME helps support this requirement by validating that only users with appropriate security rights are granted access to the system. Additionally, as users’ roles change, the FactoryTalk View ME system provides for user security right management.</td>
</tr>
<tr>
<td>j)</td>
<td>The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, to deter record and signature falsification.</td>
<td><img src="#" alt="Yes" /> <img src="#" alt="No" /> <img src="#" alt="N/A" /></td>
<td>Customers should implement policies and procedures that outline the significance of electronic signatures, regarding individual responsibility, and the consequences of falsification for both the company and the individual.</td>
</tr>
<tr>
<td>k)</td>
<td>Use of appropriate controls over systems documentation including: A comprehensive system can be implemented using FactoryTalk AssetCentre software and services. FactoryTalk View ME user documentation is provided in electronic (.pdf) format on the product CD. The distribution of these documents is at the customer’s discretion.</td>
<td><img src="#" alt="Yes" /> <img src="#" alt="No" /> <img src="#" alt="N/A" /></td>
<td>Rockwell Automation assists with controlled delivery and distribution of the correct versioning of the documents.</td>
</tr>
<tr>
<td>1</td>
<td>Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.</td>
<td><img src="#" alt="Yes" /> <img src="#" alt="No" /> <img src="#" alt="N/A" /></td>
<td>All FactoryTalk View ME documents are bundled and delivered with the product. Rockwell Automation assists with delivery and distribution of the correct versioning of the documents.</td>
</tr>
<tr>
<td>2</td>
<td>Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.</td>
<td><img src="#" alt="Yes" /> <img src="#" alt="No" /> <img src="#" alt="N/A" /></td>
<td>Rockwell Automation assists with delivery and distribution of the correct versioning of the product documents.</td>
</tr>
</tbody>
</table>

### §11.30 Controls for Open Systems

<p>| Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to assist with the 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 assist with, as necessary under the circumstances, record authenticity, integrity, and confidentiality. | <img src="#" alt="Yes" /> <img src="#" alt="No" /> <img src="#" alt="N/A" /> | Customers are responsible for establishing internal policies and procedures to assist with the appropriate controls that are put in place to meet regulation for an open system. Access to FactoryTalk View ME requires appropriate login and password regardless of whether customers choose to implement a closed or an open system. The FactoryTalk View ME Data Model and RecipePlus functions use proprietary format files and cannot be accessed with outside tools. FactoryTalk View ME v8.20 and later includes a CSVDatalog ActiveX control for capturing data to a CSV file. The CSVDatalog control CSV file includes metadata that allows a utility to detect tampering. |</p>
<table>
<thead>
<tr>
<th>Section</th>
<th>Requirements</th>
<th>FactoryTalk View ME 10.00 meets?</th>
<th>Application notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>§11.50</td>
<td>Signature Manifestations</td>
<td>Yes, No, N/A</td>
<td>FactoryTalk View ME audit trail logs actions performed by the operator and is comprised of a time and date stamp, operator ID, and the action taken.</td>
</tr>
<tr>
<td>a)</td>
<td>Signed electronic records shall contain information associated with the signing that clearly indicates the following:</td>
<td>[ ] Yes [ ] No [ ] N/A</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>The printed name of the signer;</td>
<td>[ ] Yes [ ] No [ ] N/A</td>
<td>FactoryTalk View ME audit trail records the date and time associated with each operator action.</td>
</tr>
<tr>
<td>2</td>
<td>The date and time when the signature was executed; and</td>
<td>[ ] Yes [ ] No [ ] N/A</td>
<td>FactoryTalk View ME audit trail records the action performed by the operator and approver role.</td>
</tr>
<tr>
<td>3</td>
<td>The meaning (such as review, approval, responsibility, or authorship) associated with the signature.</td>
<td>[ ] Yes [ ] No [ ] N/A</td>
<td>Audit log viewers show the user, time, and action. These fields are available for use in any reports created from the data using a third-party tool.</td>
</tr>
<tr>
<td>4</td>
<td>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).</td>
<td>[ ] Yes [ ] No [ ] N/A</td>
<td></td>
</tr>
<tr>
<td>§11.70</td>
<td>Signature/Record Linking</td>
<td>Yes, No, N/A</td>
<td>All records are automatically tied to a specific user identity reflecting who performed each action.</td>
</tr>
<tr>
<td></td>
<td>Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to provide confidence that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.</td>
<td>[ ] Yes [ ] No [ ] N/A</td>
<td></td>
</tr>
<tr>
<td>Table 2: Subpart C – Electronic Signatures</td>
<td>Section</td>
<td>Requirements</td>
<td>FactoryTalk View ME 10.00 meets?</td>
</tr>
<tr>
<td>§11.100</td>
<td>General Requirements</td>
<td>Yes, No, N/A</td>
<td>When using Windows-linked users and groups in FactoryTalk Security this requirement is met through Active Directory configuration and policy.</td>
</tr>
<tr>
<td>a)</td>
<td>Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.</td>
<td>[ ] Yes [ ] No [ ] N/A</td>
<td>When using native FactoryTalk Security users and groups, the FactoryTalk Security system enables the creation of a unique native FactoryTalk login and password for each user. The system can be configured to persist deleted user accounts to help prevent account reuse.</td>
</tr>
<tr>
<td></td>
<td>Procedures should be implemented to confirm that user IDs do not get shared or reassigned.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b)</td>
<td>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.</td>
<td>[ ] Yes [ ] No [ ] N/A</td>
<td>The customer’s management procedure should include the verification of the identity of an individual before sanctioning an individual’s electronic signature.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Once a user has been sanctioned and a unique account with a password has been created in the FactoryTalk View ME system, the user is required to enter his login and password to access FactoryTalk View ME. This process validates the identity of the user to FactoryTalk View ME.</td>
</tr>
</tbody>
</table>
### Section 11.200 Electronic Signature Components and Controls

**a)** Electronic signatures that are not based on biometrics shall:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>FactoryTalk View ME 10.00 meets?</th>
<th>Application notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Electronic signatures that are not based on biometrics shall:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1a. Employ at least two distinct identification components such as an</td>
<td>Yes</td>
<td>FactoryTalk View ME requires two components for user identification: a unique login ID and password.</td>
</tr>
<tr>
<td>identification code and password.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>1b. When an individual executes a series of signings during a single,</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>continuous period of controlled system access, the first signing shall be</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>executed using all electronic signature components: subsequent signings</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>shall be executed using at least one electronic signature component that</td>
<td></td>
<td></td>
</tr>
<tr>
<td>is only executable by, and designed to be used only by, the individual.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. When an individual executes one or more signings not performed during an</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>continuous period of controlled system access, each signing shall be</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>executed using all electronic signature components.</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

**1**. Electronic signatures that are not based on biometrics shall:

- **c)** Persons using electronic signatures shall, before 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.
  - Yes
  - No
  - N/A
  - Application notes: Customers are responsible for notifying the FDA of their intention of recognizing the electronic signature to be a legally binding equivalent of traditional handwritten signatures.

- **1**. The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.
  - Yes
  - No
  - N/A
  - Application notes: Customers are responsible for submitting the certification to the FDA that the electronic signatures in their system are intended to be a 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.
  - Yes
  - No
  - N/A
  - Application notes: Customers are responsible for any requested follow-up of certification or testimonial to have the electronic signatures be a legally binding equivalent of traditional handwritten signatures.

- **3**. Be used only by their genuine owners; and
  - Yes
  - No
  - N/A
  - Application notes: The customer is responsible for confirming that the genuine owner is signing the electronic signature and that the password is not being disclosed to others.

- **4**. Be administered and executed to provide confidence that attempted use of an individual’s electronic signature by anyone other than its genuine owner requires the collaboration between two or more individuals
  - Yes
  - No
  - N/A
  - Application notes: The customer should implement appropriate procedures to handle situations that require an electronic signature by anyone other than its genuine owner.
<table>
<thead>
<tr>
<th>Section</th>
<th>Requirements</th>
<th>FactoryTalk View ME 10.00 meets?</th>
<th>Application notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>b)</td>
<td>Electronic signatures based on biometrics shall be designed to provide confidence that they cannot be used by anyone other than their genuine owners.</td>
<td>❑ Yes ❑ No ❑ N/A</td>
<td>FactoryTalk View ME does not support biometric devices.</td>
</tr>
<tr>
<td>§11.300 Controls for Identification Codes/Passwords</td>
<td>Persons who use electronic signatures based on the use of identification codes in combination with passwords shall employ controls to provide confidence that their security and integrity. Such controls shall include:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>a)</td>
<td>Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.</td>
<td>❑ Yes ❑ No ❑ N/A</td>
<td>FactoryTalk View ME can use FactoryTalk Security or Microsoft Windows security to manage user accounts. FactoryTalk Security and Microsoft Windows security maintains all login IDs to help prevent reuse or reassignment of previously created login IDs. A user’s identification can be disabled or inactivated without deleting the user’s login ID.</td>
</tr>
<tr>
<td>b)</td>
<td>Confirming that identification code and password issuances are periodically checked, recalled, or revised (for example, to cover such events as password aging).</td>
<td>❑ Yes ❑ No ❑ N/A</td>
<td>FactoryTalk View ME can use FactoryTalk Security or Microsoft Windows security to manage user accounts. Password expiration, password aging, password complexity requirements, account expiration, disabling of accounts, lockout after n invalid login attempts, and forcing a change of password on the first login are all security features provided by both Microsoft Windows security and FactoryTalk Security.</td>
</tr>
<tr>
<td>c)</td>
<td>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.</td>
<td>❑ Yes ❑ No ❑ N/A</td>
<td>The customer is responsible for implementing loss management procedures.</td>
</tr>
<tr>
<td>d)</td>
<td>Use of transaction safeguards to help 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.</td>
<td>❑ Yes ❑ No ❑ N/A</td>
<td>FactoryTalk View ME can use FactoryTalk Security or Microsoft Windows security mechanisms to detect unauthorized use if rules for authorized use are maintained. For example, a rule might stipulate that after three incorrect login attempts an account is locked. Login attempts, whether successful or not, are logged by the system.</td>
</tr>
<tr>
<td>e)</td>
<td>Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to help verify that they function properly and have not been altered in an unauthorized manner.</td>
<td>❑ Yes ❑ No ❑ N/A</td>
<td>The customer’s management procedures should include periodic test and/or validation of any devices that may risk the integrity of a user’s identification.</td>
</tr>
</tbody>
</table>
Applying PanelView Plus 6/7 and FactoryTalk View ME in a 21 CFR Part 11 Controlled Environment

The following topics describe how PanelView Plus 6/7 and FactoryTalk View ME v10.00, or later, can be used or configured to technically satisfy the requirements of the FDA 21 CFR Part 11 regulation.

- Limit physical access to computer hardware
- Take advantage of Microsoft Windows Active Directory
- Configure the system to use Windows-linked user accounts
  - User account password aging and management
  - Managing Windows-linked security configuration in a running application
  - Configure Windows Active Directory authentication on the PanelView Plus 6/7 terminal
- Configure the system to use FactoryTalk Security user accounts
  - User account password aging and management
  - Managing native FactoryTalk users and groups in a running application
- Application design to enable 21 CFR Part 11 compliance
  - Configure runtime security-codes access codes
  - Configure system operator inactivity action
  - Configure electronic signature
  - Require operators to log in to use the system
  - Logging operator activity
  - Detecting audit and alarm circular buffer capacity conditions
  - Exporting system audit and alarm information
  - Capturing process data
  - Detecting changes in exported CSV files
  - Clearing the Alarm and Audit History buffers
  - Limit access to Configuration Mode and Shutdown buttons.
  - Supporting remote access to the application
- Control Microsoft Windows CE desktop access on PanelView Plus 6/7 terminal
- Use of the PanelView Plus 6/7 screensaver password
- Use version control software


**Limit Physical Access to Computer Hardware**

It is essential to limit operator access to the PanelView Plus 6/7 hardware running FactoryTalk View ME. In general, an operator's only access to the terminal should be via the keypad or touchscreen. An operator with access to the power switch and PanelView Plus 6/7 terminal could access the underlying file system and could potentially circumvent many of the security measures described in this document. Put measures in place to limit operator access and to help protect your hardware systems.

**Take Advantage of Microsoft Windows Active Directory**

FactoryTalk View ME uses FactoryTalk Security as its underlying security system. FactoryTalk Security is part of the FactoryTalk Services Platform. FactoryTalk Security provides local FactoryTalk users and groups, and the ability to integrate the authentication subsystem with a Windows Active Directory for centralized management of users and groups. The PanelView Plus 6/7 terminal can be configured to authenticate user accounts that are members of a Windows 2003 Server, Windows Server 2008, Windows Server 2012, or Windows Server 2016 Active Directory. It is strongly recommended that applications requiring 21 CFR Part 11 compliance utilize the ability to integrate FactoryTalk Security with a Microsoft Windows Active Directory to simplify system validation and centralize management activities.

**Configure the System to Use Windows-linked User Accounts**

Security rights in FactoryTalk View Machine Edition are managed in the Runtime Security component. Before you can configure the FactoryTalk View ME Runtime Security component, you have to create user accounts and user groups in FactoryTalk Security.

To add Windows-linked groups to FactoryTalk Security from the FactoryTalk View ME Explorer window, go to System > Users and Groups > User Groups. Right-click and select New and then Windows-linked Group to add a domain group.

When using Windows-linked groups it is recommended that the Windows-linked group(s) are configured as members of native FactoryTalk groups. To add a native FactoryTalk group from the FactoryTalk View ME Explorer window:

1. Go to System > Users and Groups > User Groups.
2. Right-click and select New, then User Group to add a native FactoryTalk Security group.
3. Add the Windows-linked groups as members of the native FactoryTalk group.

After the native FactoryTalk groups are added in the Runtime Security system, the next step is to grant A through P security codes to the Runtime Security groups.
Using groups in this manner can simplify the system validation process, as the security rights of the native FactoryTalk groups are validated. A written policy can be used to specify how individual user accounts are moved from one Windows-linked group to another.

**Use Windows Account Password Aging and Management**

When using Windows-linked groups or Windows-linked user accounts, password management and aging are configured and managed by the Windows Active Directory system administrator. Windows Active Directory user accounts and passwords should be configured so that the passwords expire after a certain time span, and accounts will lock after multiple failed login attempts. This configuration is usually specified as part of a corporate IT department Standard Operating Procedure (SOP).

**Managing Windows-linked Security Configuration in a Running Application**

Over time a company will experience a change in its workforce. Using Windows-linked accounts and Windows-linked groups provides the most flexible system, from the HMI application perspective, as nearly all aspects of security management are made at the domain level. FactoryTalk View ME v8.00 and later includes user management controls that allow for Windows-linked groups to be added to, and removed from, the system as a function of the runtime application. Please note that the Security Codes (A-P) of any group or user account cannot be modified at runtime; only native FactoryTalk Security group membership can be modified.

The Windows-linked user accounts and Windows-linked groups must be made members of native FactoryTalk Security groups that have been assigned Security Codes (A-P) in Runtime Security. Note that it is not possible to modify the attributes, such as disabling an account, or properties, such as password, of an individual’s Active Directory user account with the runtime user management controls built-in to FactoryTalk View ME. These changes must be made from a computer within the Windows Active Directory. When used, all runtime user management controls generate audit messages. Additionally, in v8.20 and later, the runtime user management controls include the ability to enable an electronic signature function.

**Configure Windows Active Directory Authentication on the PanelView plus 6/7 Terminal**

To authenticate Windows-linked user accounts in Microsoft Windows 2008, 2012, or 2016 Active Directory it is necessary to configure the PanelView Plus 6/7 terminal to use LDAP as the authentication service.

To configure the terminal, from ME Station home screen, go to Terminal Settings > Network and Communications > LDAP Configuration.

When using LDAP Over SSL Authentication it is necessary to manually transfer a security certificate from the Active Directory to the terminal.

Configure the System to Use FactoryTalk Security User Accounts

In FactoryTalk View ME, security rights are managed in the Runtime Security component. Before you can configure the FactoryTalk View ME Runtime Security component, you must create user accounts and groups in FactoryTalk Security.

To add native FactoryTalk Security groups to FactoryTalk Security from the FactoryTalk View ME Explorer window, go to System > Users and Groups > User Groups. Right-click and select New and then User Group.

After native FactoryTalk groups are created, you can add user accounts to the system. From the FactoryTalk View ME Explorer window, go to System > Users and Groups > Users. Right-click and select New, then User. The native FactoryTalk user account can be added to an existing FactoryTalk user group.

Later, once the native FactoryTalk groups are added in the Runtime Security system, the next step is to grant A through P security codes. Using user groups rather than granting rights to individual user accounts can simplify the system validation process, as the security rights of the native FactoryTalk groups are validated, and written policy can be used to specify how individual user accounts are moved from one native FactoryTalk group to another.

Use FactoryTalk Security Account Password Aging and Management

User account and password management and aging can be performed for native FactoryTalk Security user accounts. FactoryTalk Security user accounts and passwords should be designed so that the passwords expire after a certain period, and accounts lock after multiple failed login attempts. This information is usually part of a corporate IT department Standard Operating Procedure (SOP).

For applications that use native FactoryTalk user accounts, or a combination of Windows-linked and native FactoryTalk Security user accounts, FactoryTalk Security user account and password management and aging is configured as part of FactoryTalk Security. In the FactoryTalk View Studio Explorer window, go to System > Policies > Security Policies > Security Policy and double-click.

Configure Account and Password Policy to meet the application needs and SOP requirements.
Managing Native FactoryTalk Users and Groups in a Running Application

Over time a company will experience a change in its workforce. To accommodate this inevitable change, FactoryTalk View ME v8.00 and later includes user management controls that allow for native FactoryTalk Security user accounts to be added, removed, and modified in the running HMI application. The Security Codes (A-P) of any group or user account cannot be modified at runtime; only native FactoryTalk Security group membership can be modified.

It is also important to note that a newly added native FactoryTalk Security user account must be made a member of an existing native FactoryTalk Security group that has been assigned Security Codes (A-P) in Runtime Security before the user can successfully log in to the application. Using the runtime user management controls, it is possible to modify the user account attributes, like account lockout status, and properties, like password or group membership. When used, all user management controls generate an audit message. Additionally, in v8.20 and later, the user management controls can be configured to use the electronic signature function.

Application Design to Enable 21 CFR Part 11 Compliance

Configure FactoryTalk View Runtime Security Codes for Security Accounts

Whether the application uses Windows-linked user accounts, native FactoryTalk Security user accounts, or a combination, after the user accounts and user groups have been created in FactoryTalk Security, they must be added to the Runtime Security editor in FactoryTalk View ME. When adding a user group or user account, assign the security codes that give the account access to secured HMI components. These codes run from A through P and determine which displays a user has rights to at runtime.

If a user account or user group of which the user is a member is not added to Runtime Security, the user will not be able to log in to the system.

When adding groups or users while the application is running, it is important to keep this in mind - until the new member or group is added to a group configured in Runtime Security, the new member or members will not be able to log in. It is not possible to assign or change A-through-P security codes during runtime. Please refer to the section Managing users and groups from the running application.

Security codes are assigned as dictated by the application’s security design. If a user account is a member of multiple groups configured in Runtime Security, the user account will be assigned the most restrictive set of A through P security codes.
To restrict access to a graphic display, assign a security code to it using the Display Settings dialog. Only users who have been granted the assigned A through P code can access the display.

Configure System Operator Inactivity Action

Operators should never allow anyone else to perform operations using their credentials. To help prevent this, the application can be configured to automatically log out the current user after a period of operator inactivity. For added security, the system can also be configured to navigate to a selected display immediately or after an additional delay.

Require Operators to Login to Use the System

The application must be designed to help prevent the default user account, DEFAULT, from modifying data or accessing displays that contain critical process information. This can be accomplished using the security codes A through P and configuring displays to restrict access. This requires operators to log in to the system before any operational actions, for example, a process variable change, can be completed.

Additionally, when a control is configured to use the electronic signature feature, the DEFAULT user account is prohibited from making a data change using that control.
Require Reverification of Operator Identity, or Supervisor Signoff

Some applications require “reverification” of the operator’s identity to complete specific critical operations, or even an additional supervisory signoff as part of their procedures. FactoryTalk View ME provides this level of security through its electronic signature and authorization capability.

When using this functionality, operators are prompted to enter their electronic signature (system password), and, if configured, obtain verification from an “approver,” before a setpoint (tag value) can be changed. These actions, both the operator’s and approver’s, generate audit messages. The message logged includes time occurred, username, old value, new value, operator comments regarding why the change was made, and who approved the change.

Appendix A lists all graphic controls that support the electronic signature function. Each control is configured uniquely. Examples of the audit trail generated by the electronic signature function can be found in The FactoryTalk View Studio for Machine Edition User Guide.

The electronic signature audit messages are in addition to the ‘standard’ audit message generated by operator actions, for example:

**Example: Operator accepts an action and approver approves the action**

In the countersignatory mode, when the operator accepts an action, and the approver approves the action, the system generates the following audit messages:

Electronic Signature Action: Write ‘225’ to the tag ‘Curing Delay’. Previous value was ‘200’. Proposed by ‘Jim’. Comment: Humid day requires a longer material cure.

Electronic Signature Action: Proposed Write ‘225’ to the tag ‘Curing Delay’. Previous value was ‘200’. Approved by ‘Emil’. Comment: Agree with Jim’s assessment of humidity.
Logging Operator Activity

The system automatically generates operator action audit-trail information. PanelView Plus 6/7, and MobileView can all be configured to forward operator activity audit messages to a FactoryTalk AssetCentre system for centralized storage. It is not possible for ME Station running on a computer to forward operator activity messages to a central FactoryTalk AssetCentre System.

FactoryTalk View ME v10.00 introduces a local ‘onboard’ storage of operator activity audit messages. This feature can be enabled regardless of the hosting platform; onboard audit message storage is supported both on PanelView Plus 6/7 and by ME Station running on a computer. Onboard audit message storage can also be used along with FactoryTalk AssetCentre, so that audit messages are stored locally and passed to FactoryTalk AssetCentre. It is important to note that the local audit message storage does not operate as a store-and-forward cache. That is, the local ‘onboard’ audit storage does not solve the lost message problem that occurs when connectivity between the PanelView Plus 6/7 and FactoryTalk AssetCentre is lost.

Capturing Operator Activity in the Local Onboard Audit Trail

To capture operator activity in the local onboard storage, the Audit Trail feature must be enabled and the size of the circular buffer must be set. The circular buffer can store from 500 to 10,000 audit messages.

Audit trail is enabled in the Startup properties for the application and enables operator actions to be captured in the local onboard audit trail. Enabling the Audit trail option will start the audit service when the application is executed. This setting is set at design-time and cannot be changed from the runtime environment. The setting is part of the runtime file (MER), and cannot be disabled or circumvented.

When the Audit trail option is enabled, only v10.00, and later, runtime MER files can be created for the application.
When local onboard auditing is enabled, Operator activity audit messages are stored locally in a circular buffer. The buffer size can be set from 500 to 10,000 messages. The default is 2,000 messages. Once the maximum size of the buffer is reached, the next message will overrun the buffer and begin overwriting the oldest audit message. The Audit Trail Setup editor is accessed from the Project Explorer tree.

Please carefully review the section in this document on detecting audit and alarm circular buffer capacity conditions.

Capturing Operator Activity in a Central FactoryTalk AssetCentre System

To capture and store operator activity audit messages in a central FactoryTalk AssetCentre system, the PanelView Plus 6/7 terminal and FactoryTalk Diagnostics system must be properly configured. To configure FactoryTalk Diagnostics, launch the FactoryTalk® Administration Console, and select the Network scope when prompted. This must be done from a computer that is a member of the same network-scope FactoryTalk Directory as the FactoryTalk AssetCentre server.

When the FactoryTalk Administration Console opens, select Tools > FactoryTalk Diagnostics > Setup. Next, select Destination Setup and enable the checkbox Enable this computer to receive messages broadcast from Windows CE devices or MobileView.

Then, select Message Routing and the Secured message type and enable the checkbox Accept message from Windows CE devices.

You will need to record the IP address of the computer where FactoryTalk Diagnostics was configured. Also, record the port number if it was changed from the default.
To configure the PanelView Plus 6/7 terminal, from the ME Station home screen, navigate to Terminal Settings > Diagnostics Setup. Select Remote Log and click Edit. **Address** is the IP address of the computer configured to accept messages from Windows CE devices, and **Port** is the communication port configured on the same server. The default is 4445.

Rockwell Automation Knowledgebase article 58977 can be referenced for step-by-step instructions.

Please note that FactoryTalk Services on the PanelView Plus 6/7 forwards operator audit trail messages directly to the FactoryTalk AssetCentre system. There is no local buffering or caching of the operator audit messages. If connectivity to the FactoryTalk AssetCentre system is lost, the forwarded operator audit messages will be lost and will not be stored in the FactoryTalk AssetCentre system database.

**Detecting Local Onboard Audit and Alarm Circular Buffer Capacity Conditions**

Both the local onboard alarm and audit histories are stored in circular buffers. This results in special consideration for which the application’s standard operating procedures must account. FactoryTalk View ME v10.00 adds circular buffer capacity warnings and overrun detection for both the alarm and audit history circular buffers. When one of the capacity/overrun conditions is met, the configured tag will be set to ‘true’ (nonzero); this information can be used in the HMI application to warn the operator that the local onboard buffer is approaching its capacity. For example:

- The capacity flag could be used to generate an alarm in the built-in HMI Alarm system, or
- A visibility animation on a banner object, used in all displays, could show the banner when the capacity flag is ‘true’, informing the operator of the situation.

The *High and High-high* capacity warnings use a configurable setpoint for detection. The default thresholds for the high capacity and high-high capacity warning are 90% and 99% respectively. When the number of messages in the buffer exceeds the setpoint multiplied by the buffer size, the flag will be set to ‘true’ (nonzero). The **Capacity Overrun** flag is set when the system begins to overwrite the oldest data after the maximum capacity of the buffer is reached.
In this example, the maximum number of audit messages is set to 10,000, the high capacity warning is set to 90%, and the high-high capacity warning is set to 98%, the system will:

- Set the **High capacity** tag when the 9,001st message is written to the buffer.
- Set the **High-high capacity** tag when the 9,801st message is written to the buffer.
- Set the **Capacity Overrun** tag when the 10,001st message is written to the buffer.

Capacity warnings and overrun detection have been added to the alarm subsystem in FactoryTalk ME v10.00. The Advanced tab, within the Alarm Setup editor, includes the tag connections to configure the High Capacity, High-high Capacity, and Capacity Overrun for the alarm history circular buffer.

Please note, when the audit or alarm history is cleared using the Clear Audit History or Clear Alarm History buttons, or cleared remotely via tag connection, the High Capacity, High-high Capacity, and Capacity Overrun flags are reset to ‘false’ (zero).

**Exporting Local Onboard Application Audit and Alarm Information**

FactoryTalk View ME v10.00 adds the capability to export the contents of the local onboard Alarm, Audit, and Diagnostic historical information to a CSV file. This capability can be incorporated into an application’s standard operating procedure to export and store the process information being logged to the local onboard alarm and audit buffers. This export capability is especially useful when a buffer’s content exceeds the high or high-high capacity setpoint, and the process needs to continue logging audit and alarm information. The exported information can also be processed with external applications to create an electronic batch record.
The CSV Export Setup editor is accessed from the Project Explorer. The CSV Export Setup configuration is made at design-time and cannot be changed within the running application. It is necessary to enable the feature and select which information to export. By default the feature is disabled.

The storage path is a constant and does not support the use of a string tag to change the path dynamically. The system does not support a UNC path (i.e.\<servername\>\<sharename\>).

Tag connections are used to trigger the export. The Export Trigger could be an HMI tag used in a button in the HMI application, thus relying on the operator to export the history files, or the Export Trigger could be a controller tag that is set by the control system.

The File Label connection allows for a unique identifier to be added to the exported filenames (ex. a batch id).

Finally, the Status connections allow the system to communicate the results of an export operation to the system.

Since the Alarm, Audit, and Diagnostic history files use different schemas, when the export occurs, each selected “Type” generates a separate CSV file. Each file contains a date and time stamp in the file name, and if configured the string contained in the “File Label” connection. It is important to know that when an export is triggered, the date and time stamp in the file name will be the same for all exported files. Each file also contains the name of the source: Alarm, Audit, or Diagnostic. For example, for information exported on 25.Sept.2017 triggered at 2:30:11 with a “File Label” connection of “Batch_187”, the files would be named:

- 2017_09_25_14_30_11-Batch_187-ALARM.CSV
- 2017_09_25_14_30_11-Batch_187-AUDIT.CSV
- 2017_09_25_14_30_11-Batch_187-DIAGNOSTIC.CSV

The CSV files contain the entire content of the Alarm, Audit, or Diagnostic history files at the time the export was executed.

After exporting the Alarm and Audit files, it would be the normal operation to clear the circular buffers.

**Clearing the Audit or Alarm History Buffers**

When the process dictates, or the alarm or audit history circular buffers become full, it may be necessary to empty the circular buffers. Emptying the circular buffers can be accomplished through the operator, by including buttons in the application, or by the control system through tag connections.

Before emptying the alarm or audit buffers their contents should be exported to CSV file ensuring the preservation of the information stored in the buffers. Standard operating procedures should stipulate that the buffers should be emptied only after a successful export operation.
The application must include a Clear Alarm History or Clear Audit Trail buttons to enable an operator to empty the associated buffer. Both button's electronic signature capability is enabled by default; helping prevent the default user account, DEFAULT, from emptying the buffers. When an operator empties either buffer an audit message is generated. It should be noted, when the audit trail circular buffer is emptied the first audit message in the newly emptied audit buffer records the identity of the user that emptied the audit trail circular buffer.

Emptying the alarm or audit history circular buffers remotely, via a tag, does not generate an audit message.

**Capturing Process Data**

FactoryTalk View ME features two different methods to collect process data: the Data Log Model, and the CSVDataLog ActiveX control.

The Data Log Model uses a circular buffer that can store up to one million total data points of historical data. The Trend control uses the Data Log Model as its data source to present historical data to the operator, via a line chart. The process data in the Data Log Model is stored in a proprietary format. The proprietary file can be transferred to a PC and converted to Microsoft Excel format using a utility. The Data Log Model uses a circular buffer; this means that when the buffer becomes full, the oldest data is overwritten with new data added to the buffer. The circular buffer aspect of the Data Log Model may make it unsuitable as a data collection mechanism in some applications.

A more suitable solution for data collection uses the new CSVDataLog ActiveX control available with FactoryTalk View Machine Edition v8.20 and later. This control provides data sampling at a maximum frequency of 250 ms, stores data in a CSV file, and provides tamper detection functionality designed to help an application comply with 21 CFR Part 11. When tamper detection is enabled, the CSV file generated by the logging function contains *data integrity metadata*. This metadata allows a companion desktop utility to detect whether an outside data source has modified CSV data. The *Enable Tamper Detection* property is enabled by default when an instance of the CSVDataLog control is created.

The CSVDataLog control can be configured to generate a new CSV file periodically. The CSV file name can be date and time-stamped to help identify when the file was created.
Detecting Changes in Exported CSV Files

FactoryTalk View Studio for Machine Edition v8.20 and later includes a standalone utility that can be used to perform tamper detection on CSV files exported by a running Machine Edition application. The CSV files generated when exporting the Alarm, Audit Trail, or Diagnostics History files, or by the CSVDataLog ActiveX control include information that allows the utility to detect inter- and intra-line changes in the CSV file being analyzed. Detecting altered CSV files allows the application to comply with 21 CFR Part 11 Section §11.10 and §11.30.

Limit Access to Configuration Mode and Shutdown Buttons

The application should use the available security options, electronic signature, Security Codes (A-P) or expression security functions to limit which users can access the Shutdown and Configuration Mode buttons. Both buttons halt the execution of the HMI application.

- The Configuration Mode button stops the HMI application and returns to the ME Station home screen.
- The Shutdown button stops the execution of both the HMI application and ME Station, giving the user direct access to the Microsoft Windows CE desktop.

Supporting Remote Access to the Application

Remotely accessing the running application can be helpful in many instances. For example, remotely connecting to a system to troubleshoot or diagnose an operational issue. Remote access to PanelView Plus 6/7 applications can be accomplished via Virtual Network Computing (VNC) or FactoryTalk ViewPoint. Each presents challenges to systems that must comply with 21 CFR Part 11.
Virtual Network Computing (VNC)

VNC supports a remote connection to the terminal that directly controls the application. That is, the remote user and the local operator share a session. VNC supports read-only and read-write modes. In the read-write mode, both the local and remote user can interact with the terminal. Therein lies the problem from a 21 CFR Part 11 compliance perspective. When a user is remotely connected via VNC the system cannot differentiate between the remote and local user. This causes two compliance issues:

1) Since the system cannot differentiate between the local and remote user, it is possible that the recorded username is incorrect. For example, Bob logs in remotely to VNC (read-write mode). Next, Bob logs into the application. At the same time, Sam is standing in front of the same PanelView Plus terminal. Sam changes a tag value in the system. The operator action audit message recorded from Sam’s action will be attributed to Bob since Bob is the current logged in user.

2) The system cannot identify the location (terminal or remote device) that initiated an action. For example, Mary logs in remotely to VNC (read-write mode). At the same time, Owen is standing in front of the same PanelView Plus terminal and logs in to the application. Mary remotely changes a tag value in the system. The operator action audit message recorded from Mary’s action will show the location as the terminal’s name, not the remote device’s name.

It is recommended that when an application must comply with 21 CFR Part 11, VNC is disabled, or limited to read-only mode.

FactoryTalk ViewPoint

Unlike VNC, FactoryTalk ViewPoint supports one remote connection to an application instance. The application instance can be the same displays the operator uses, a set of unique displays solely accessible to the FactoryTalk ViewPoint user, or a combination of displays. FactoryTalk ViewPoint has three operational modes: read-only, permission-based security, and full control. Full Control mode allows any remote user to make read-write changes in the application without requiring the user to log in. Full Control mode should not be used in an application that must comply with 21 CFR Part 11.

When using permission-based security, the remote user’s ability to perform a read-write action is based on the security configuration for the user group of which the remote user is a member.

It is important to note that FactoryTalk ViewPoint uses a separate security instance. When an application is launched, both FactoryTalk View ME and FactoryTalk ViewPoint security configuration is synchronized. However, if the runtime security management tools available in FactoryTalk View ME are used to alter the security configuration, those changes are not used by FactoryTalk ViewPoint.

Example 1, Joe is a new employee that has been added to the running application as a member of the Operators group. Although Joe can log in to the terminal, Joe will not be able to log in to FactoryTalk ViewPoint successfully.

Example 2, Cindy is an operator that has been promoted. The admin changes Cindy’s group membership in the running application from Operators to Supervisors. When Cindy logs in to the application on the terminal, she will have all permission granted in the Supervisors group. However, when Cindy logs in remotely to FactoryTalk ViewPoint, Cindy will still only have the Operators group permissions.
The security challenges can be mitigated by using Windows-linked groups, by either explicitly granting access to the Windows-linked group, or by using Windows-linked groups that are members of local FactoryTalk security groups. When configuring the system using Windows-linked groups that are members of local FactoryTalk security groups, please note that the behaviors described above using one user account also apply to the Windows-linked groups.

**Example 3,** Joe is a member of a new Windows-linked group Third_Shift_Operators. The Windows-linked group has been added to the running application as a member of the Operators group. Although Joe can log in to the terminal, Joe will not be able to log in to FactoryTalk ViewPoint successfully.

**Example 4,** Windows-linked Group_A is moved from the Operators FactoryTalk security group to the Maintenance FactoryTalk security group. When a member of Group_A logs on to the terminal, the user will be granted access based on the configuration for the Maintenance group. When a member of Group_A logs in remotely to FactoryTalk ViewPoint, the user will have permissions configured for the Operators group.

These security configuration considerations notwithstanding, FactoryTalk ViewPoint will generate operator action audit messages when tag values are changed remotely. The actions are properly attributed to the remote user logged in to the FactoryTalk ViewPoint application instance. The audit messages are stored in the onboard auditing circular buffer.

Due to the security considerations described above for systems that must comply with 21 CFR Part 11, it is recommended that FactoryTalk ViewPoint be used in read-only mode.

### Control Microsoft Windows CE Desktop Access on PanelView plus 6/7 Terminal

Desktop Access is a feature that allows for controlled access to the Microsoft Windows CE desktop on a PanelView Plus 6/7 terminal. Access to the desktop should be controlled to help prevent unauthorized changes to the operating system. Operating system modifications do not generate audit messages.

During initial out-of-the-box power-on of a PanelView Plus 6/7 terminal, v8.10 and later, the system prompts for a Desktop Access password and Challenge Question/Answer pair. Setting this information is not optional. Later, it is possible to set the terminal to Allow desktop access.

If these initial values are lost or forgotten, there is no ‘backdoor.’ The terminal must be reset to ‘Factory Default’ so these items can be set to known values.
When Desktop Access is set to Disallow, the user will be prompted to enter the password before they are able to exit ME Station and access the Microsoft Windows CE desktop.

If the application standard operating procedures allow, Desktop Access can be set to Allow, permitting the user to exit ME Station without entering a password at any time.

**Use of the PanelView Plus 6/7 Password-enabled Screensaver**

Although Microsoft Windows CE 6.0 provides a password-protected screensaver, it is recommended that the screensaver password protection is not used in an application that must comply with FDA 21 CFR Part 11. When the screensaver is active the system only supports one common password that is shared by all users to unlock the terminal. Instead of using the password-protected screensaver, the system should use the operator inactivity automatic logout feature.

**Use Version Control Software**

FactoryTalk AssetCentre can be used to keep track of revisions to your FactoryTalk View ME v8.00, and later, projects. FactoryTalk AssetCentre provides preferred integration with FactoryTalk View ME and other Rockwell Software products. Version control software such as FactoryTalk AssetCentre retains all project components in a central repository for safekeeping. To modify any portion of the project, a user must check out the component. The version control software logs the username, component, and checkout date and time. The user modifies the component in FactoryTalk View ME, closes FactoryTalk View ME, and then checks the component back in. The version control software logs the username, component, and check in date and time, and allows the user to add comments explaining the modifications. This provides you with a record of all changes you made and when you made them. You also have access to both the old and new versions of the checked out component.
About Rockwell Automation

Rockwell Automation, Inc. (NYSE: ROK), the world’s largest company dedicated to industrial automation and information, makes its customers more productive and the world more sustainable. Headquartered in Milwaukee, Wis., Rockwell Automation employs about 20,000 people serving customers in more than 80 countries.

Publishing Application Notes

This document includes detailed recommendations for developing FactoryTalk View Machine Edition applications that comply with the U.S. government’s 21 CFR Part 11 regulation. Rockwell Automation publishes documentation in the Literature Library, which can be accessed at http://www.rockwellautomation.com/global/literature-library/overview.page

References


Appendix A – FactoryTalk View Machine Edition Objects Supporting Electronic Signature

The following graphic objects support electronic signature operation in FactoryTalk View Machine Edition 8.20, and later:

- Numeric and String:
  - Numeric Input Cursor Point button
  - Numeric Input Enable button
  - String Input Enable button

- Push Button:
  - Maintained Push button
  - Multistate Push button
  - Ramp button
  - Interlocked Push button
  - Latched Push button

- Alarm:
  - Acknowledge Alarm button
  - Acknowledge All Alarms button
  - Clear Alarm History button
  - Reset Alarm Status button

- User Management:
  - Add User/Group button
  - Delete User/Group button
  - Modify Group Membership button
  - Unlock User button
  - Enable User button
  - Disable User button
  - Password button
  - Change User Properties button

- Advanced:
  - Shutdown button
  - Macro button
  - Control List Selector
  - Piloted Control List Selector
  - Go to Configure Mode button

- RecipePlus:
  - RecipePlus button

- Audit
  - Clear Audit Trail button (10.00)