FactoryTalk® View Site Edition (SE)
Complying with 21 CFR Part 11: Electronic Records & Signatures

Guidelines for applying
FactoryTalk View SE in a 21 CFR Part 11 environment

Doc ID FTALK-WP003C-EN-E
# Table of Contents

FactoryTalk® View Site Edition (SE) ........................................................................................................... 1

Introduction .................................................................................................................................................. 5

Defining Key Terms .................................................................................................................................... 6

FactoryTalk View SE in a Rockwell Automation software system ............................................................... 7
  FactoryTalk View SE and the FactoryTalk® Services Platform ................................................................. 7
  How FactoryTalk® AssetCentre fits in ...................................................................................................... 7

Complying with the Part 11 Regulation ....................................................................................................... 8

Applying FactoryTalk View SE in a 21 CFR Part 11 controlled environment ............................................. 14
  Limit physical access to computer hardware ......................................................................................... 14
  Use NTFS or other secure file system ..................................................................................................... 14
  Take advantage of operating system security and domains ................................................................. 14
  Take advantage of the FactoryTalk View Site Edition architecture .................................................... 15
  Configure FactoryTalk View SE user accounts to use Microsoft Windows security ......................... 15
  Remove FactoryTalk View runtime security codes for all user accounts ............................................. 15
  Use a password-protected screen saver ................................................................................................ 16
  Configure FactoryTalk View SE clients to automatically log out .......................................................... 17
  Prohibit access to FactoryTalk View Studio and other software programs ......................................... 17
  Use Windows account password aging and management ................................................................... 17
  Use log on requirements for computers in a FactoryTalk View SE environment ................................ 18
  Set up the DeskLock feature .................................................................................................................. 18
  Do not allow operator access to Help ..................................................................................................... 19
  Secure FactoryTalk View SE Active Display Client stations .................................................................. 20
  Log all FactoryTalk View SE activity and alarms to a central ODBC/SQL database ............................ 21
Create an ODBC data source to serve as a central database ................................................................. 22
Configure FactoryTalk® Diagnostics to track activity ............................................................................. 23
Configure the FactoryTalk View SE Alarm Log ......................................................................................... 24
Configure the FactoryTalk View SE Data Log ............................................................................................ 26
Set up a SQL Server or Oracle database .................................................................................................. 28
Set up re-verification of operator identity, or supervisor signoff .............................................................. 28
Configuration of the FactoryTalk View SE Signature Button .................................................................. 30
Use version control software .................................................................................................................... 33
About Rockwell Automation ....................................................................................................................... 34
Participation in PDA Part 11 Task Group .................................................................................................. 34
Completing internal gap analysis ............................................................................................................. 34
Publishing application notes ...................................................................................................................... 34
References ................................................................................................................................................ 34
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 lieu of handwritten signatures and records executed on paper. The scope of this regulation, 21 CFR Part 11, is significant and impacts all computer systems related to the manufacturing of a life science product (e.g. 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 is calculated 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.

FactoryTalk View Site Edition (SE) can enable life science manufacturers to cost-effectively comply with Part 11 while achieving optimal operational and regulatory compliance efficiencies. A software product in itself cannot be “compliant” with the electronic records and signatures portion of 21 CFR Part 11, but when applied properly, FactoryTalk View SE can help meet the needs of customers who are required to comply with these regulations.

The purpose of this document is to provide life science manufacturers with a description of how FactoryTalk View SE addresses 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 medical manufacturers and has created a solution that is flexible enough to address these differences. The objective is to help medical manufacturers quickly and cost-effectively comply with Part 11, while opening up new competitive advantage opportunities.
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 upon 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 SE in a Rockwell Automation software system

FactoryTalk View SE and the FactoryTalk® Services Platform

FactoryTalk View SE uses the FactoryTalk Services Platform (FTSP), a set of software components and services that are shared by many Rockwell Automation software products. FTSP allows applications to be developed that share definitions, administration and real-time data. For FactoryTalk-enabled systems, this means that tags need only be created one time; once tags are created in a PLC program, for example, those tags can then be used directly in FactoryTalk View SE without having to create and maintain a separate tag database.

In a typical HMI system (without FTSP), a PLC programmer would add a new tag to the PLC program. Details about this new tag would need to be recorded and its usage would need to be documented. A separate tag would also need to be added to the HMI system; details about this tag would again need to be recorded and its usage documented in the HMI system. With FTSP, when the new tag is added to the controller logic program, it is immediately available to FactoryTalk View SE – there is no need to add it separately to the HMI tag database.

FTSP provides FactoryTalk software products with FactoryTalk® Diagnostics, which offers a consistent, reliable means for Rockwell Software products to communicate and pass messages back and forth. This allows for the logging of event, audit and alarm messages from FactoryTalk View SE and all other FactoryTalk-enabled products to a centralized, common data store.

An FTSecurity-enabled system allows for one-time security configuration. This means that once users and user groups have been created, all FTSecurity-enabled software products can make use of those same users and user groups. Creating and disabling or deleting accounts, configuring security rights, and grouping users into similar categories all need only be done once for the entire system. FTSecurity-enabled products can also be linked with Microsoft Windows security, further streamlining the configuration of users and user groups.

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.

The intent of this document is to describe how to use FactoryTalk View SE to secure and log operator actions, track alarms, and log other operational data. FactoryTalk AssetCentre is not discussed in detail. Refer to the FactoryTalk AssetCentre Validation Package for requirements and specifications for compliance with 21 CFR Part 11.
Complying with the Part 11 Regulation

21 CFR Part 11 is made up of two major subparts (regarding 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 help provide confidence that products like FactoryTalk View SE comply with the technical aspect of Part 11. Each customer’s security and standard operating procedures (SOP) for supporting this regulation are unique. FactoryTalk View SE is flexible and configurable to meet the various SOPs and implementations needed to facilitate this regulation. See tables 1 and 2 for more information on 21 CFR Part 11 and how the general functionality of FactoryTalk View SE applies.

Table 1: Subpart B – Electronic Records

<table>
<thead>
<tr>
<th>Section</th>
<th>Requirements</th>
<th>FactoryTalk View SE applies?</th>
<th>Application notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>§11.10</td>
<td>Controls for closed systems</td>
<td>□ Yes □ No □ N/A</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>All records are stored in an SQL-compliant ODBC database. FactoryTalk View SE provides tools to read locally buffered records, but once they have been sent to the ODBC database and removed from the local buffer, users can use a standard reporting tool such as Microsoft Access, Microsoft SQL Server tools, or Crystal Reports to read the records.</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>All records are stored in an SQL-compliant ODBC database and are available for viewing, printing, and exporting throughout the records retention period. Precautionary measures such as periodic backup of the database are procedures that customers should incorporate into their SOP.</td>
<td></td>
</tr>
<tr>
<td>c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.</td>
<td>□ Yes □ No □ N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Section</td>
<td>Requirements</td>
<td>FactoryTalk View SE applies?</td>
<td>Application notes</td>
</tr>
<tr>
<td>---------</td>
<td>--------------</td>
<td>-----------------------------</td>
<td>------------------</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 SE to use Microsoft Windows security. It also includes using other security measures, such as FactoryTalk View SE security and FactoryTalk View SE Desk Lock, which prevent unauthorized access to data files or 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. 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>With the FactoryTalk View SE Signature Control, each entry into the FactoryTalk View SE activity log is identified with the time and date the action occurred and the name of the logged-in operator who performed the action, as well as the type of operation that was performed and the values of the changed item before and after the change. If electronic signatures are used, the operator’s username and full name are also included.</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 a combination of controller logic and FactoryTalk View SE. FactoryTalk View SE supports both screen-level and tag-level security. An application can be developed to support user-initiated operational checks, which require screen security.</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 SE uses a combination of Microsoft Windows domain security and FactoryTalk View SE security. Customers should implement policies and administrative procedures to define authorized access to the system.</td>
</tr>
<tr>
<td>h)</td>
<td>Use of device (e.g. terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.</td>
<td>☐ Yes □ No □ N/A</td>
<td>FactoryTalk View SE uses functions such as login and password to validate the source of data input. Location-specific security settings can enforce “line of sight” by allowing certain operations only from designated terminals that are within visual range of machinery.</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>☐ Yes □ No □ 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 SE helps support this requirement by validating that only users with appropriate security rights are granted access to the system.</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, in order to deter record and signature falsification.</td>
<td>□ Yes ☐ No □ N/A</td>
<td>Customers should implement policies and procedures that outline the significance of electronic signatures, in terms of individual responsibility, and the consequences of falsification for both the company and the individual.</td>
</tr>
<tr>
<td>Section</td>
<td>Requirements</td>
<td>FactoryTalk View SE applies?</td>
<td>Application notes</td>
</tr>
<tr>
<td>---------</td>
<td>--------------</td>
<td>------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>k)</td>
<td>Use of appropriate controls over systems documentation including:</td>
<td></td>
<td>A comprehensive system can be implemented using FactoryTalk AssetCentre software and services. FactoryTalk View SE user documentation is provided both in electronic (.pdf) format on the product CD and hard copy format. The distribution of these documents is at the customer’s discretion.</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>☐ Yes □ No □ N/A</td>
<td>All FactoryTalk View SE documents are bundled and delivered with the product. Rockwell Automation assists with controlled 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>☐ Yes □ No □ N/A</td>
<td>Rockwell Automation assists with delivery and distribution of the correct versioning of the product documents.</td>
</tr>
<tr>
<td>§11.30</td>
<td>Controls for open systems</td>
<td></td>
<td>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 SE requires appropriate login and password regardless of whether customers choose to implement a closed or an open system.</td>
</tr>
<tr>
<td>§11.50</td>
<td>Signature manifestations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>a)</td>
<td>Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:</td>
<td></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 SE provides an audit trail for actions performed that is minimally comprised of a time and date stamp, operator ID and full name, and the action taken. The customer should include the full name of the user in any reports.</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 SE records the date and time associated with each action in the activity logs.</td>
</tr>
<tr>
<td>Section</td>
<td>Requirements</td>
<td>FactoryTalk View SE applies?</td>
<td>Application notes</td>
</tr>
<tr>
<td>---------</td>
<td>--------------</td>
<td>-----------------------------</td>
<td>-------------------</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>The FactoryTalk View SE Signature run time dialog box can be configured to display and record the meaning of the signature. It also allows for separate performer and approval signatures, and for comments to be added regarding the meaning of the signature.</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>The FactoryTalk View SE activity log viewer shows the user name, 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>§11.70</td>
<td>Signature/record linking</td>
<td>☒ Yes ☐ No ☐ N/A</td>
<td>All signatures and records are automatically tied to a specific user to identify who performed each action. Data records in the ODBC data store should be protected by a user name and password, thus preventing information from being altered.</td>
</tr>
<tr>
<td>Table 2: Subpart C – Electronic Signatures</td>
<td>§11.100 General requirements</td>
<td>☒ Yes ☐ No ☐ N/A</td>
<td></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>The FactoryTalk System Administration tool can enable the creation of a unique login and password for each user. Procedures should be implemented to ensure that user IDs do not get deleted or reassigned.</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 prior to sanctioning an individual’s electronic signature. Once a user has been sanctioned and a unique account with password has been created in the FactoryTalk View SE system, the user is required to enter his login and password to access FactoryTalk View SE. This process validates the identity of the user to FactoryTalk View SE.</td>
</tr>
<tr>
<td>c)</td>
<td>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.</td>
<td>☐ Yes ☒ No ☐ N/A</td>
<td>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.</td>
</tr>
<tr>
<td>1.</td>
<td>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.</td>
<td>☐ Yes ☒ No ☐ N/A</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Section Requirements

<table>
<thead>
<tr>
<th>Section</th>
<th>Requirements</th>
<th>FactoryTalk View SE applies?</th>
<th>Application notes</th>
</tr>
</thead>
</table>
| 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 | 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. |

### §11.200 Electronic signature components and controls

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

| 1.      | Employ at least two distinct identification components such as an identification code and password. | □ Yes  
□ No  
□ N/A | FactoryTalk View SE requires two components for user identification: a unique login ID and password. |
|---------|-------------------------------------------------|------------------|--------------------------------------------------|
| 1.a.    | 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. | □ Yes  
□ No  
□ N/A | FactoryTalk View SE requires the complete user identification – unique login ID and password – in the initial login of the application.  
When using the FactoryTalk View SE Signature Control, both the user login ID and password are required to perform an action.  
If the user logs out of FactoryTalk View SE and again requires access, the user must re-enter the login ID and password. |
| 1.b.    | 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. | □ Yes  
□ No  
□ N/A | The customer must implement logout procedures to enforce user log off at the end of any continuous period of controlled system access, and to enforce log on at the start of the next access period. To ensure that a workstation is not left unattended, a password-protected screensaver should be used for all FactoryTalk View SE clients.  
FactoryTalk View SE can support the use of all electronic signature components where required and as mandated in the customer’s SOP. |

**b)** Electronic signatures based upon biometrics shall be designed to provide confidence that they cannot be used by anyone other than their genuine owners.

| 2.      | Be used only by their genuine owners; and | □ Yes  
□ No  
□ N/A | The customer is responsible for ensuring that the genuine owner is signing the electronic signature and that the password is not being disclosed to others. |
|---------|-------------------------------------------|------------------|--------------------------------------------------|
| 3.      | Be administered and executed to provide confidence that attempted use of an individual’s electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals. | □ Yes  
□ No  
□ N/A | The customer should implement appropriate procedures to handle situations that require an electronic signature by anyone other than its genuine owner. |
| b)      | Electronic signatures based upon biometrics shall be designed to provide confidence that they cannot be used by anyone other than their genuine owners. | □ Yes  
□ No  
□ N/A | FactoryTalk View SE can support interfaces to biometric-based logon mechanisms. |
<table>
<thead>
<tr>
<th>Section</th>
<th>Requirements</th>
<th>FactoryTalk View SE applies?</th>
<th>Application notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>§11.300</td>
<td>Controls for identification codes/passwords</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 SE can use Microsoft Windows security to manage user accounts. Microsoft Windows security maintains all login IDs to 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>Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).</td>
<td>☐ Yes ☐ No ☐ N/A</td>
<td>FactoryTalk View SE can use 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 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 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 SE can use 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 suspended. FactoryTalk View SE also provides the ability to use VBA code to create a login macro or button action that requires the operator to enter a separate piece of information or answer a question to validate the login ID. The user’s response can be examined in VBA code to determine whether the login ID and password are being used improperly. If so, the information can be reported immediately to system security and/or management.</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 ensure that they function properly and have 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 FactoryTalk View SE in a 21 CFR Part 11 controlled environment

The following topics describe how FactoryTalk View SE can be used or configured to technically satisfy the requirements of the FDA 21 CFR Part 11 regulation.

- Limit physical access to computer hardware
- Use NTFS or other secure file system
- Take advantage of operating system security and domains
- Take advantage of the FactoryTalk View SE architecture
- Configure FactoryTalk View SE user accounts to use Microsoft Windows security
- Remove FactoryTalk View SE runtime security codes for all user accounts
- Use a password-protected screen saver
- Configure FactoryTalk View SE clients to automatically log out
- Prohibit access to FactoryTalk® View Studio and other software programs
- Use Windows account password aging and management
- Use log on requirements for computers in a FactoryTalk View SE environment
- Set up the DeskLock feature
- Do not allow operator access to Help
- Secure FactoryTalk View SE Client stations
- Log all FactoryTalk View SE activity and alarms to a central ODBC/SQL database
- Set up re-verification of operator identity, or supervisor signoff
- Use version control software

Limit physical access to computer hardware

It is essential to limit operator access to the hardware running Windows operating systems and FactoryTalk View SE. In general, an operator's only access to the computer should be via the keyboard, mouse, or touch screen. An operator with access to the power switch and bootable media could have direct access to 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 protect your hardware systems.

Use NTFS or other secure file system

Depending on your application, you can limit operator access and rights to parts of the file system by using NTFS. FAT and FAT32 are not secure file systems.

Take advantage of operating system security and domains

FactoryTalk View SE makes efficient use of the security features built into the underlying Microsoft Windows operating systems. For compliance, all FactoryTalk View SE computers in a closed system must be part of the same Windows domain. All FactoryTalk View SE computers must run Windows Vista Business, Windows 2008 Server,

**Take advantage of the FactoryTalk View Site Edition architecture**
FactoryTalk View SE servers run as services and therefore do not require any user to be logged on to the FactoryTalk View SE server computer. Operators can log in and out of the FactoryTalk View SE client stations without affecting the computer or software components of the FactoryTalk View SE servers. Windows password aging and management can be used at the clients while the servers are running a continuous operation. Operators at the FactoryTalk View SE client stations have no way to alter server processes or shut down the server operation. Even if server components are run on the same computer that an operator is using, these components run as services in the background, and are not affected by the security permissions of whoever happens to be logged onto the computer.

**Configure FactoryTalk View SE user accounts to use Microsoft Windows security**
Before you can add users and user groups to the accounts list in the FactoryTalk View SE Runtime Security editor, you have to create accounts for them in FactoryTalk Security services. In the FactoryTalk View SE Explorer window, right-click **System > Users and Groups** and select **Security**. Click **Add**, then click the **Create New** button and select **Windows linked user group** or **Windows linked user**, depending on whether you have chosen to show groups or users. Add only a subset of the Microsoft Windows users to FactoryTalk View SE, as needed. When you start a FactoryTalk View SE project that uses the Windows Security option, the current Windows user is logged into FactoryTalk View SE if that user has been added to the FactoryTalk Security users list.

The Windows-linked All Users group is automatically added to the FactoryTalk Runtime Security accounts. By default, this gives all users access to all FactoryTalk View SE run-time security codes (A-P), and all FactoryTalk Security actions. If you want to restrict access to the FactoryTalk system, you need to remove the All Users account, create FactoryTalk security accounts for the users and computers you want to secure, and then assign them the appropriate security permissions.

**Remove FactoryTalk View runtime security codes for all user accounts**
After you create users and user groups in FactoryTalk® Security, you add them to the security accounts list in the Runtime Security editor in FactoryTalk View SE. When you add an account, you also assign the security codes that will give them access to secured HMI components. These codes run from A-P and determine which components a user has rights to at run time.

To restrict access to a command, macro, graphic display, OLE object verb, or HMI tag, you assign a security code (from A-P) to it, and then assign that code only to users who should have access to the component.
By default for all new projects, all FactoryTalk View SE runtime security codes are assigned to all user accounts. To remove security code assignments, clear the Allow check box for FactoryTalk View Security Codes for the All Users group:

You must then assign the runtime security rights to users and user groups as required for each project.

**Use a password-protected screen saver**

To ensure that a workstation in a closed system is not left unattended, use a Windows XP/2000 password-protected screen saver for all FactoryTalk View SE clients. To configure screen savers, from the Windows Control Panel, select Display, and click the Screen Savers tab. Add password protection to the screen saver.

Because FactoryTalk View SE server components run as services, with no need for an interactive Windows user to be logged on, it is not necessary to use password-protected screen savers on the FactoryTalk View SE HMI server or FactoryTalk® Directory computer.
Configure FactoryTalk View SE clients to automatically log out
For some installations, a password-protected screen saver on each client machine is not enough protection. In these cases, FactoryTalk View SE clients can be configured to automatically log out after a specified period of time. This will log them out of FactoryTalk View SE client, not out of their Windows session.

![FactoryTalk View SE Client Auto Logout](image)

To log a user out automatically when the keyboard or mouse is inactive for a period of time, enable auto logout, and then enter the inactivity period.

- **Enable auto logout**
- **Inactivity period:** 10 minutes

Prohibit access to FactoryTalk View Studio and other software programs
FactoryTalk View Studio is not intended for use by operators. They should not be given access to FactoryTalk View Studio. The easiest way to do this is to not install FactoryTalk View Studio on operator computers. If it is necessary to install FactoryTalk View Studio on these computers, it should be secured using DeskLock.

Use Windows account password aging and management
User account and password management and aging are done in Microsoft Windows by the system administrator. User accounts and passwords should be set up so that the passwords expire after a certain time and with appropriate lockouts after multiple failed login attempts. This information is usually part of a corporate IT department Standard Operating Procedure, or SOP. For more information, refer to your Windows documentation.

An operator at a FactoryTalk View SE client can log off FactoryTalk View SE and Windows without affecting the FactoryTalk View SE servers or other parts of the system. Where possible, operators should be required to log out of Windows when not using the FactoryTalk View SE client.
Use log on requirements for computers in a FactoryTalk View SE environment
Each user must log on to the Windows 2000 or XP computer at the start of their session, and log off when they are done. Since the FactoryTalk View SE server components run as services, it is not necessary to have any user logged on to computers which are used as an HMI Server or FactoryTalk Directory server. Operators should not use FactoryTalk View SE servers as operator stations.

Computers that are used as FactoryTalk View SE display clients must have the actual operator log on to the computer. Operators should never allow anyone else to perform operations using their user name and password. If it is necessary for a supervisor to perform or approve certain operations, a different computer should be used, or the Signature Button tool should be used. If the same computer is used, the operator should log off Windows, and the supervisor should log on. In cases where two signatures are required (i.e., operator and supervisor), the approval will take place through the use of a Signature Button feature while the operator remains logged in to the system.

The FactoryTalk View SE client should also be configured to automatically log the current user out and close all displays after a period of mouse or keyboard inactivity.

Set up the DeskLock feature
To ensure that operators remain within a closed environment while running FactoryTalk View SE, use the DeskLock feature. Used in conjunction with disabling switching to other applications and other security configurations noted in the DeskLock documentation, it is possible to lock operators into a closed FactoryTalk View SE runtime system. The
DeskLock tool and accompanying documentation are available from the FactoryTalk View Tools, which are installed with the FactoryTalk View SE software.

**CAUTION.** Do not implement the DeskLock feature without first carefully reading the documentation. DeskLock can have far-reaching effects on your operating system. Its purpose is to replace the standard Windows desktop with a customized one intended to prevent operators from having access to operating system functionality, such as restarting Windows or shutting down tasks. If you do not leave a way for the administrator to access this functionality, there could be no access to it at all. DeskLock also configures Windows Policies.

**Do not allow operator access to Help**

The Windows Help system is not secure, and once in help, a user can get full access to the underlying file system (still limited by their Windows account). Do not allow operators to have access to Windows or FactoryTalk View SE Help.

Help can be restricted by using a combination of DeskLock and overriding the F1 help keys in the FactoryTalk View SE application. It can also be restricted using Windows security on the help executables.
Secure FactoryTalk View SE Active Display Client stations
Configure clients with the following settings in the FactoryTalk View SE client wizard (settings should be as shown).

- **Do not allow display code debugging.** This will allow the launching of the VBA editor, which is not secure.
In the FactoryTalk View SE Client Window Properties dialog box select **Disable switch to other applications**, and **Maximize window**:

- **Show title bar**—enable only if necessary.
- **Show System menu and close button** – disable to prevent operators from closing window.
- **Maximize window**—enable; prevents operators from seeing or clicking items on the desktop.
- **Show Diagnostics List** – enable only if necessary.
- **Disable switch to other applications**—enable; prevents operators from switching to other applications.

In addition, use the DeskLock tool on the computer running the FactoryTalk View SE Client and configure it to launch only the FactoryTalk View SE client window.

**Log all FactoryTalk View SE activity and alarms to a central ODBC/SQL database**

To ensure the integrity of FactoryTalk View SE activity data while still providing a backup if the central database is temporarily unavailable, use the Central Logging ability of FactoryTalk View SE. If the central database is temporarily unavailable, the local logs serve as backup buffers until the central database connection is restored.

Note that FactoryTalk View SE’s own log file viewers will only access the information in the local buffer files, not the historical information that has been sent to the central database.
To use this system, follow the steps below to:

- create an ODBC data source to serve as the central database
- configure FactoryTalk Diagnostics to track activity
- configure the FactoryTalk View SE Alarm Log
- configure the FactoryTalk View SE Data Log
- set up a Microsoft SQL Server or Oracle database.

Create an ODBC data source to serve as a central database

To create an ODBC data source, follow the instructions in the FactoryTalk View SE documentation, or you can configure it from Windows Control Panel > Administrative Tools > Data Sources (ODBC). The following steps assume that a Microsoft SQL Server database is being used.

1. On the System DSN tab, click Add to create a new data source.
2. Scroll through the list of drivers and select SQL Server. Click Finish.
3. Respond to prompts from the wizard to create a new data source to SQL Server. When you finish typing your entries, click Next.
4. At the next window, select the option, “With Windows NT authentication using the network login ID.” Click Next.

5. Continue working through the wizard, selecting options and clicking Next. When you finish, test the communications to your new ODBC data source. This ODBC data source can now serve as the central data source.

**Configure FactoryTalk® Diagnostics to track activity**

The following steps must be performed on each machine that will be a FactoryTalk View SE client.

1. From the FactoryTalk View Studio Tools menu, open the Diagnostics Setup editor.
2. Under Destination Setup, select Local Log to configure settings for the local log on this computer.
3. Leave the Logging path at its default. Make sure the maximum log size is large, for example 25,600 KB. Overwrite events as needed.
4. Select ODBC Database to configure settings for logging to the central ODBC data source.
5. For Message Buffering, log messages to the database every two minutes or less, and buffer messages locally for at least 12 hours.
6. Configure the ODBC data source to point to the SQL Server or other ODBC data source you configured earlier. Maintain connections for at least twice as long as the logging period, or indefinitely.
7. If you configured the ODBC data source database to allow NT Authentication, you do not need to enter login information.
8. Select Message Routing to specify which categories of messages should be routed to each logging destination (local log or ODBC data source).
Configure the FactoryTalk View SE Alarm Log

1. From the FactoryTalk View Studio Tools menu, open the HMI Tag Alarm Log Setup editor.

2. On the Logging tab, leave the default settings.

3. On the File Management tab, configure settings to start a new alarm log file weekly, and delete the oldest files after 3 weeks.

Note that this is not deleting records from the central database, but rather information from the local buffer. This should only be done after the information has already been sent to the central database. While it is possible to configure it to never delete these buffer files, realize that this would eventually fill up the hard drive unless some other method were used to delete files.
4. On the Central Logging tab, enable periodic central logging every two minutes or less. Configure the ODBC data source to point to a SQL Server, Oracle, or other database. Configure it to maintain connections for at least twice as long as the logging period, or indefinitely. The login information does not need to be specified if the database allows NT Authentication, otherwise a valid database user ID and password must be specified.
5. In the Alarm Setup editor, configure each severity to log to the alarm log file. Logging alarms to the printer is optional.

Configure the FactoryTalk View SE Data Log
If your application requires Data Logging, you should log to a secure ODBC database.

1. From the FactoryTalk View SE Application Explorer, open the Data Log Model for your HMI Server.

2. On the Setup tab, select ODBC database as the storage format.
3. On the Paths tab, configure an ODBC backup path.

If the connection to the ODBC database is temporarily broken, backup information will be kept in this location. This location must be secured using the operating system security or using DeskLock so that operators cannot modify the files. When the ODBC database becomes available again, the DatalogMergeToPrimary command must then be used to merge the backup data into the primary database. This can be done by running the DatalogMergeToPrimary every day using Event Detector, or through written Standard Operating Procedures.
4. On the File Management tab, do not configure purging of old records. All management of historical records should be handled in the ODBC database.

Set up a SQL Server or Oracle database
These instructions are beyond the scope of this paper. For help, refer to your database documentation.

Set up re-verification of operator identity, or supervisor signoff
Once an operator is logged on to Windows and FactoryTalk View SE client, all operations are logged with the user name. Some companies have a “re-verification” of operator identity for specific crucial operations, or specific supervisor signoff as part of their procedures. FactoryTalk View SE provides this level of security through its signature and authorization capability. When using this functionality, users are prompted to enter their electronic signature and obtain verification from a supervisor, if needed, before trying to perform a set-point change or command. These activities are then logged to the FactoryTalk View SE activity log and any external ODBC log. The information logged includes username, old value, new value, operator comments regarding why the change was made, and who approved the change.

At run time the click of the button will present a window in which the new value of the tag can be entered. This window also provides the place where an electronic signature, in the form of a username and password, is entered to confirm the identity of the operator that is performing the change. The approval of the operation can require that an approver will also enter an electronic signature. The window provides space for a user comment about the operation.
to be entered. Any of these options can be enabled or disabled through the signature button property pages or through the FactoryTalk View SE property panel.

All electronic signature authentication and required information, such as a comment and valid data range, is validated before the tag value is written or the command is issued. If a username or password is incorrect at runtime, the value will not be changed and a warning message will be shown. If an option is enabled, then information must be entered for that option; a warning message will be shown if any information is left blank. FactoryTalk View SE will log any information about the tag write and any warnings or errors to the activity log.

The log entry will record the name of the user who made the change, the original value of the tag, what it was changed to, who approved it, and any comment that was entered. The prefix "ESign:" is configurable, and the format of the information message is shown in the following example:

ESign: Operation: Change Temp Setpoint, value change for 'Tag1' from 35 to 50. Performed by OperatorID OPERATOR FULLNAME. Approved by SupervisorID SUPERVISOR FULLNAME, Comment: changed per order 345B.
Configuration of the FactoryTalk View SE Signature Button
1. Add the signature button control to a FactoryTalk View graphic by clicking the Objects Menu and selecting ActiveX Control. Draw a rectangle on the graphic for the button and then select the "FactoryTalk View SE Signature Button" from the ActiveX objects list.

![Insert an ActiveX Control]

2. If you want to see the value of the set point to verify the change, add a numeric display to the graphic. Link the numeric display with the tag whose set point will be downloaded.

3. Save the graphic. Give it a unique name in the application.

4. Double-click the Signature Button to open the custom property pages to configure it. Configure settings on each tab as follows:
General tab

- Enter a caption for the button

Signature tab

- Select the operation the button will perform, then set Min and Max values and # of decimal places displayed
- Check to enable authentication of the performer of the action, then enter the user group the performer must be in
- Check to enable an approver authentication, then enter the user group the approver must be in
5. Click OK to close the Signature Button Properties dialog box.

6. Under the Tools menu, configure the Diagnostics Setup to show the result of tag writes in the activity bar of FactoryTalk View Studio. Set the FT View Diagnostics List message categories as follows:

7. You can change these settings to test how messages are logged.

8. Test-run the display in FactoryTalk View Studio. Click on the Signature Button to show the FactoryTalk View Electronic Signature runtime dialog window and fill in the information fields that pop up. You must have the user groups set up and be logged in as a user that is a member of the designated “performer” group to initiate the action.
Check the activity bar to see the entries documenting successful and unsuccessful set point changes.

9. Close the graphic when you are done testing the signature button.

10. To test the display in the client, configure a FactoryTalk View SE client.

Use version control software

FactoryTalk AssetCentre can be used to keep track of revisions to your FactoryTalk View SE projects. FactoryTalk AssetCentre provides preferred integration with FactoryTalk View SE and other Rockwell Software products. Version control software such as FactoryTalk AssetCentre retains all of the 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 user name, component, and checkout date and time. The user modifies the component in FactoryTalk View SE, closes FactoryTalk View SE, and then checks the component back in. The version control software logs the user name, 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 should 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.

Participation in PDA Part 11 Task Group
The PDA (Parenteral Drug Association) formed this task group to provide a set of best practices for Part 11 compliance. This group is viewed as the authority on Part 11 compliance from an implementation perspective. The task group includes representatives from the pharmaceutical industry, suppliers to the industry, consultants, and the FDA. Rockwell is one of two automation suppliers on the task group. We have two members participating in the core group and two additional members on the extended team. Involvement in this group gives Rockwell direct access to accurate and up-to-date interpretations of the regulation and compliance practices as they evolve. We also view this opportunity as a way of adding balance to interpretations and recommended practices so that they remain practical and easily accessible by the entire pharmaceutical industry.

Completing internal gap analysis
Rockwell Automation has undertaken and nearly completed a gap analysis of most of our software products in relation to 21 CFR Part 11. In general, the software products we have evaluated have been judged as either “compliant” or “can be made compliant.” Many of our products’ standard features and complementary technologies support 21 CFR Part 11 when implemented properly.

Publishing application notes
This document includes detailed recommendations for developing FactoryTalk View SE projects that comply with the U.S. government’s 21 CFR Part 11 regulation. Rockwell is in the process of producing additional documentation that details recommended practices for product compliance. We will publish additional documentation on the Web-based Rockwell Software Knowledgebase: http://support.rockwellautomation.com.

References