Implementing Vijeo Citect to meet the requirements of FDA 21 CFR Part 11

Version 2.0 July 2008

Vijeo Citect

Background

In 1991, members of the pharmaceutical industry met with the Food and Drug Administration, (FDA), to determine how they could accommodate paperless record systems under the current good manufacturing practice (CGMP) regulations in parts 210 and 211 (21 CFR parts 210 and 211). FDA created a Task Force on Electronic Identification/Signatures to develop a uniform approach by which the agency could accept electronic signatures and records in all program areas.

The final rule provides criteria under which FDA will consider electronic records to be equivalent to paper records, and electronic signatures equivalent to traditional handwritten signatures. Part 11 (21 CFR Part 11) applies to any paper records required by statute or agency regulations and supersedes any existing paper record requirements by providing that electronic records may be used in lieu of paper records. Electronic signatures which meet the requirements of the rule will be considered to be equivalent to full handwritten signatures, initials, and other general signings required by agency regulations.

FDA 21 CFR Part 11 Requirements Summary

The requirements show the need for a secure control system to include user login, automatic logout after no user activity and procedures to ensure that the users who perform the actions on the system are both the authorized user and not an imposter. A closed system or a runtime only system is a means of securing the control system as it only allows authorized users to access and apply changes to the system.

The other major part of the requirements involves the tracking of logged data and system changes. When changes are made by a user that is required to be signed, the records can be stored electronically if the user enters proper password or uses a suitable biometric device. Data that is logged and stored has to have valid timestamp and be secure, which includes a full audit trail log of any changes that are made to the data along with backup and restore procedures.

Document Purpose

This document is a guide to how to configure Vijeo Citect to meet each requirement of 21 CFR Part 11.

Vijeo Citect can be implemented to meet the requirements of the FDA 21 CFR Part 11. It is important to understand that the Vijeo Citect cannot be validated, but rather the process implemented. Therefore, the system must still undergo the proper FDA validations to meet the requirements, including both documentation and training.

See Also

Relevant information on securing your SCADA system can be found in the product help under the section “Using Vijeo Citect / Securing Projects”.

SCADA Implementation Guidelines

The guidelines on how to implement Vijeo Citect to comply with CFR 21 Part 11 are explained in the next chapter. Step by step instructions are provided for each for the relevant subpart sections B and C of the 21 CFR 11. Requirements are listed on the left column. On the right column of the page is one of the following classifications:

FDA	The FDA has requirements regarding procedures that have to be in place to be able to obtain '21 CFR Part 11' certification from the FDA. These requirements do not directly involve the SCADA implementation.
SCADA Runtime	These sections involve deploying SCADA runtime only system for the SCADA operator consoles.
Data Logging	These sections refer to the data that is to be logged.
Security	These sections refer to system security, both SCADA and/or Windows security.
Genies	These sections refer to areas where Vijeo Citect genies and super genies will assist in developing a solution.
Commands	These sections refer to sections involving the issuing of operational commands.

Text that is in the following format is an extract from the 21 CFR Part 11 document that is relevant to the section and can help explain the intention.

Text extract from the 21 CFR Part 11 document

Note

The below chapters use the term "secure relational database" for storage of electronic records. It is important to note, that FDA does not declare the format or storage method of electronic records in 21 CFR Part 11. FDA requires the persons to "ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records". As the most advanced technology for that purpose is the use of a relational database, this document applies the term of relational database for that. However, the system can utilize other data storage means as far as the above requirements are met.

Table 1 – CFR 21 Part 11 Subpart B

21 CFR 11 – Electronic Records;
Electronic Signatures

Subpart B – Electronic Records

§ 11.10 Controls for closed systems.
Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

For a closed system implementation, a SCADA runtime only deployment is recommended with the use of proper Windows security to inhibit direct access to the file system.

On SCADA servers or client nodes: by running SCADA as the shell. On "Control" and "View-only" clients: either by running SCADA as the shell or by running a SCADA web client.

Integration of Windows security in the SCADA application helps system administrators to manage SCADA users based on corporate policies.

The SCADA application shall contain all security controlled access to data or controls to be used by the system operators ("signer" in FDA terminology). System administrators shall have security controlled access built in the SCADA application to system administration tools in Windows.

It is the customers' responsibility to ensure the system administrators have procedures to control access to the system and the runtime files by proper Windows policy setup

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

It is the customers responsibility to ensure the systems undergo the proper FDA validation procedure. The systems integrator shall be aware of the customers QMS to be able to achieve the quality targets during system design, implementation, testing and documentation.

(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.

The electronic records should be logged to a secure relational database. The data should never be deleted or destroyed but rather new records added if an authorized change is required. All logged records should include the user's security identifier and be secure.

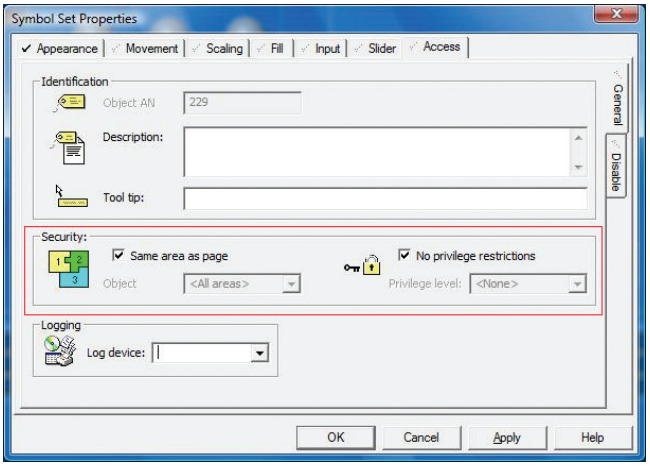
Human readable reports should be setup to display the data logged to the secure relational database and are available to be copied by the FDA.

(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

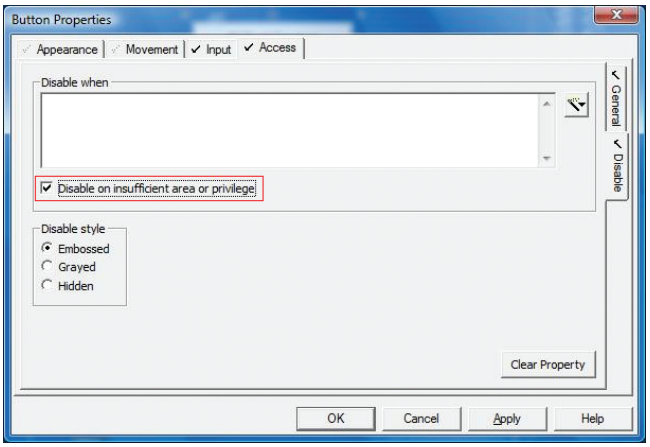
Data logged to the secure relational database should be kept for the appropriate retention period and protected via security. Suitable secure backup and restore procedures should be used.

(d) Limiting system access to authorized individuals.

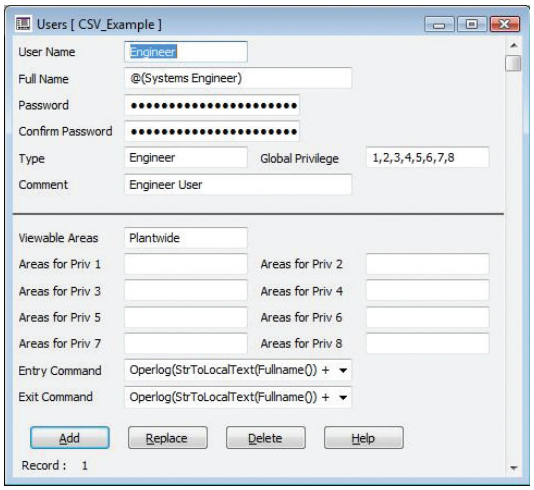
Security should be used to limit users to areas that they have the appropriate authorization level to access. Level of user access on those areas is controlled by user privileges.

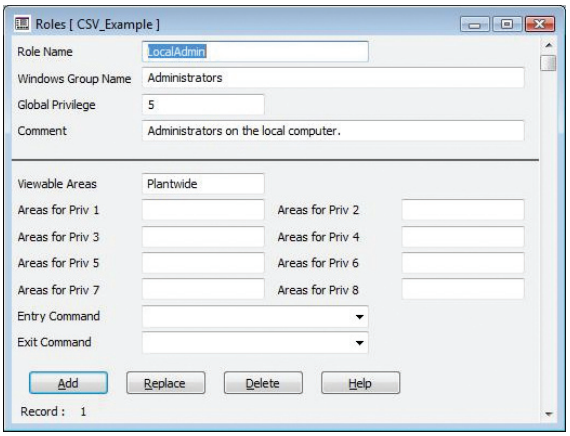


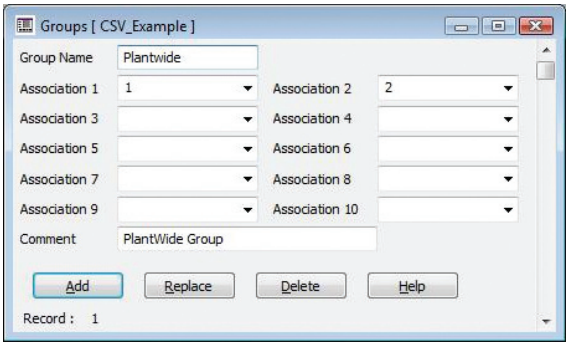
and optionally



Integrated Windows security (available from Vijeo Citect V7.10) is recommended and allows domain or workgroup level user authorization.







It is the customer's responsibility to maintain the user database and provide policies and controls to:

- use encrypted passwords
- logout a user after a time with no user activity
- control aging of passwords, minimum, maximum
- control reuse of passwords
- inhibit reuse of user accounts
- control account deletion or account inactivation
- check for user code and password length limits
- check for password strength

Successful and failed login attempts as well as logouts should be indicated in the audit trail.

The agency does not believe that it is necessary at this time to include an explicit requirement that systems be capable of detecting the absence of records. The agency advises that the requirement in § 11.10(e) for audit trails of operator actions would cover those actions intended to delete records. Thus, the agency would expect firms to document such deletions, and would expect the audit trail mechanisms to be included in the validation of the electronic records system.
It is the agency's intent the audit trail provide a record of essentially who did what, wrote what, and when.

The agency considers such operator actions as activating a manufacturing sequence or turning off an alarm to warrant the same audit trail coverage as operator data entries in order to document a thorough history of events and those responsible for such events. Although FDA acknowledges that not every operator "action," such as switching among screen displays, need be covered by audit trails, the agency is concerned that revising the rule to cover only "critical" operations would result in excluding much information and actions that are necessary to document events thoroughly.

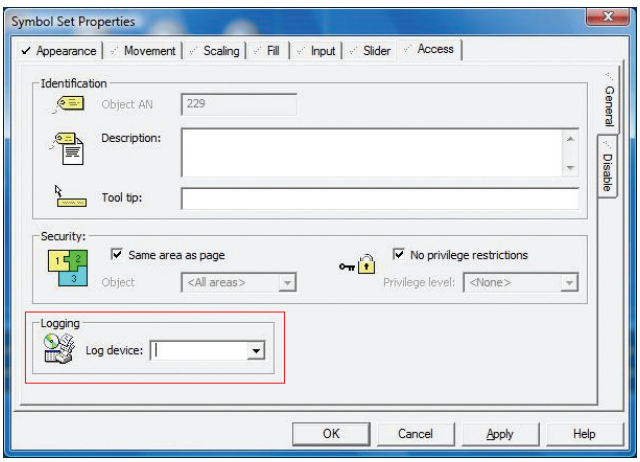
(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

When data is logged to the secure database, it should include:

- a timestamp
- node identifier
- current logged in user's security identifier or username (if username is unique between users)
- description of user action and user entered command or data.

Logged data should never be deleted or destroyed but rather new records added. In multi-node systems timeserver should be used to keep all SCADA nodes in time sync.

Use of SCADA message logs in graphic objects and Cicode based data logging shall target separate data tables to avoid record corruptions caused by unsynchronized logging processes.



Human readable audit trail report controls shall be developed to filter, merge and present message log records of multiple data sources on multiple nodes for display reports and for paper based printouts.

The audit trail shall be talkative enough to replay the relevant user activities for a selected period of time. Based on that all operator activities, which influences the process shall be logged to the secure database:

- user logins, logouts
- system startup, shutdown commands
- alarm controls
- single devices controls
- setpoint changes
- parameter changes
- operational mode changes
- sequence controls
- administration commands

The agency believes that, in general, the kinds of operator actions that need to be covered by an audit trail are those important enough to memorialize in the electronic record itself. These are actions which, for the most part, would be recorded in corresponding paper records according to existing record keeping requirements. The agency intends that the audit trail capture operator actions (e.g., a command to open a valve) at the time they occur, and operator information (e.g., data entry) at the time the information is saved to the recording media (such as disk or tape), in much the same manner as such actions and information are memorialized on paper.

The audit trail need not capture every keystroke and mistake that is held in a temporary buffer before those commitments. For example, where an operator records the lot number of an ingredient by typing the lot number, followed by the "return key" (where pressing the return key would cause the information to be saved to a disk file), the audit trail need not record every "backspace delete" key the operator may have previously pressed to correct a typing error. Subsequent "saved" corrections made after such a commitment, however, must be part of the audit trail.

The agency advises that audit trail information may be contained as part of the electronic record itself or as a separate record. FDA does not intend to require one method over the other. The word "independently" is intended to require that the audit trail not be under the control of the operator and, to prevent ready alteration, that it be created independently of the operator.

The agency advises that the purpose of performing operational checks is to ensure that operations (such as manufacturing production steps and signings to indicate initiation or completion of those steps) are not executed outside of the predefined order established by the operating organization.

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

Vijeo Citect should be configured to ensure users follow a permitted sequence of steps when operating the system. The use of Genies and Super Genies is recommended to ensure users follow the same steps during a process over the entire system. The graphical user interface shall cover all possible operational modes. The operation of Genies and Super Genies has to be validated against the functional specification. The testing and qualification process shall cover the audit trail recording and retrieval. The process control configuration tools like PLC configuration or programming tools enable low level data and functional access of the system and like those, shall not be accessible for SCADA users.

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

Vijeo Citect security (optionally with Integrated Windows Security) should be used to limit users to areas that they have the appropriate authorization level to access including operation and data logs. The customer shall establish a suitable user policy as of §11.10. (d) and the Vijeo Citect application developer shall implement the designed policies.

The Vijeo Citect systems shall be designed and implemented on a secure way to prevent unauthorized access. Networked systems with shared storage resources have to be protected against external intrusion to alter or delete data records. Similarly, remote desktop access has to be strictly controlled against unauthorized access to sensitive system resources which can result data loss or data modification by unauthorized personnel.

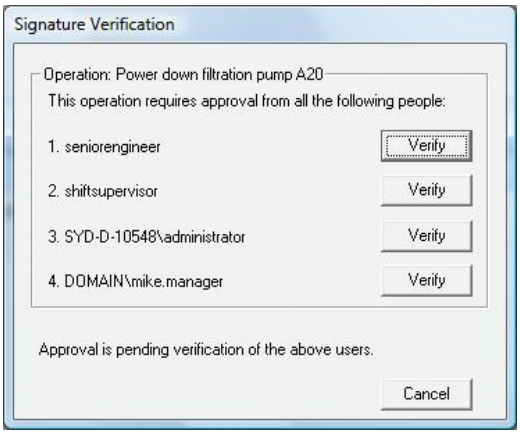
Organizations do not have to embed a list of authorized signers in every record to perform authority checks. For example, a record may be linked to an authority code that identifies the title or organizational unit of people who may sign the record. Thus, employees who have that corresponding code, or belong to that unit, would be able to sign the record. Another way to implement controls would be to link a list of authorized records to a given individual, so that the system would permit the individual to sign only records in that list.

The agency believes that these checks are warranted where only certain devices have been selected as legitimate sources of data input or commands. In such cases, the device checks would be used to determine if the data or command source was authorized. In a network, for example, it may be necessary for security reasons to limit issuance of critical commands to only one authorized workstation. The device check would typically interrogate the source of the command to ensure that only the authorized workstation, and not some other device, was, in fact, issuing the command.

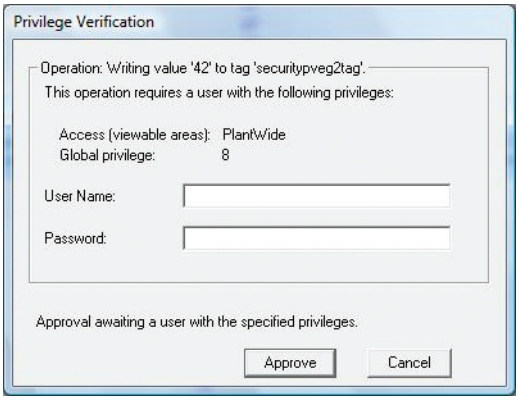
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

Operational commands should be confirmed along with the SCADA terminal location and user's area to check the validity of an operational command.

Vijeo Citect (from version 7.10 onwards) has some built in validation functions for confirming the change to a critical command or data in the system. These are: MultiSignatureForm, MultiSignatureTagWrite, PrivilegeVerifyForm and PrivilegeVerifyTagWrite.



The MultiSignature functions enforce verification of security credentials of up to four specific users (specified in the function call) before an operation is allowed to initiate.



(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

It is the customer's responsibility to ensure selected development staff has the proper skills and practical experience to deliver systems which has to be equipped with electronic record/ electronic signature system. It is also the customer's responsibility to ensure its users undergo the appropriate training to ensure correct system operation.

(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

It is the customer's responsibility to ensure suitable policies are in place to allow the use of electronic signatures by the FDA.

(k) Use of appropriate controls over systems documentation including:
(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.
(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

Product Manuals are available in pdf format on the Vijeo Citect DVD. All documentation should be controlled in regards to distribution, access and use.

Validation shall include test procedures to check the availability and completeness of operational user's manuals and maintenance manuals.

Change control procedures should be in place for system documentation.

§ 11.30 Controls for open systems.
Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure 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 ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

It is the customer's responsibility to implement procedures and controls to provide secure applications and data handling in open systems.

Vijeo Citect, like other control systems are used mainly closed systems. However there are designed for remote operation in case of need, like maintenance. The system access either has to be controlled by the corporate network access management, like utilization of secure VPN connections or by using remote access services based on secure network protocols and remote access host application running on the target system. The system design and operation has to be done with care to maintain the integrity, authenticity and confidentiality of electronic records and the remote system access has to be continuously monitored for the safe operating security conditions.

§ 11.50 Signature manifestations.
(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:
(1) The printed name of the signer;
(2) The date and time when the signature was executed; and
(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.
(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

All logged, audit and other electronic data is required to contain the following information:

- The actual name of the user along with the security identifier or username (if username is unique between users).
- The date and time.
- Additional information to provide meaning to the data. The user should be prompted when appropriate to obtain the reason for their operational action.

The electronic records should be logged to a secure relational database. The data should never be deleted or destroyed but rather new records added if an authorized change is required. All logged records should include the user's security identifier and be secure. Human readable reports should be setup to display the data logged to the secure relational database and are available to be copied by the FDA.

§ 11.70 Signature/record linking.
Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

All logged, audit and other electronic data should contain the security identifier or username (if username is unique between users) that is linked to the operation performed. SCADA security should be used to limit users to areas that they have the appropriate authorization level to access including operation and data logs.

When the logged in user executes series of commands in the Vijeo Citect system the executed actions are logged to the secure database. It is up to the customer to specify and the systems integrator to implement all or parts of data entries or commands to be confirmed individually when entering to the system. Relevant information entry can be confirmed securely at the time of information entry. This can be achieved by either requiring the username and password to be entered for validation of up to 4 user accounts (using MultiSignatureForm or MultiSignatureTagWrite), or requiring credentials from any single user that meets a specified set of privileges (using PrivilegeVerifyForm or PrivilegeVerifyTagWrite). Vijeo Citect will accept information entered only if all required user credentials entered are validated. This way the username(s) recorded in the electronic record links the account holder to their password without storing the actual password entered to the record.

The agency agrees that the word "link" would offer persons greater flexibility in implementing the intent of this provision and in associating the names of individuals with their identification codes/ passwords without actually recording the passwords themselves in electronic records.

Table 1 – CFR 21 Part 11 Subpart C

Subpart C – Electronic Signatures

	The security identifier should be unique between all users. If username is used, then it is the customer's responsibility to ensure that the username is kept unique within the system. It is recommended that no username should be ever reassigned to another individual. By using Windows Integrated Security the policies for the Vijeo Citect system can be synchronized with the corporate domain security policies to lock user accounts forever.
§ 11.100 General requirements. (a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	*Where an electronic signature consists of the combined identification code and password, § 11.100 would not prohibit the reassignment of the identification code provided the combined identification code and password remain unique to prevent record falsification. The agency believes that such reassignments are inadvisable, however, to the extent that they might be combined with an easily guessed password, thus increasing the chances that an individual might assume a signature belonging to someone else.*
(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	It is the customer's responsibility to ensure that procedures are in place to verify the identity of individuals within the system.
(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures. (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. (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.	It is the customer's responsibility to ensure systems undergo the proper FDA validation procedure. The validation documentation shall contain the register of user accounts to give access to the system at system commissioning time and, additionally the protocols to describe the controlled management of the users database during system operation.

§ 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.

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

Windows Integrated Security is recommended to be used to provide a username and password for each user.

For a user to login to the system, they will be required to use both their username and password to gain access. Subsequent system data entries should require only the password entered by the user (this is the signature component that is known only to, and usable by, the user). The username is to be remembered and stored by the Vijeo Citect application for the time the functional specification defines for "subsequent system data entries threshold". When the time expires the username has to be cleared on application level. When new data entry and the user approval is required, the empty user name forces the application to both user name and password requested to validate and execute the user command. The above procedure shall be initiated on each SCADA node as the function shall be node related.

SCADA should be set up to logout a user after a predefined time period with no user activity and procedures should be used to ensure that users do not leave the terminal unattended during their session.

(2) Be used only by their genuine owners; and

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

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

It is the customer's responsibility to ensure that electronic signatures are only used by the owner of that signature (login).

The agency advises that the intent of the collaboration provision is to require that the components of a non-biometric electronic signature cannot be used by one individual without the prior knowledge of a second individual. One type of situation the agency seeks to prevent is the use of a component such as a card or token that a person may leave unattended. If an individual must collaborate with another individual by disclosing a password, the risks of betrayal and disclosure are greatly increased and this helps to deter such actions.

Procedures are required to ensure that attempted use of someone's electronic signature requires the collaboration of two or more people.

If biometrics is used for electronic signatures, then procedures should ensure that they are only be used by the owner of that signature.

§ 11.300 Controls for identification codes/ passwords.

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

SCADA user account passwords must use encryption.

Corporate domain security policies used in conjunction with the Windows Integrated Security feature of Vijeo Citect can be used to confirm new passwords meet the minimum requirements for length, reuse,.etc listed in § 11.10 (d)

It is the customer's responsibility to ensure that the username is unique within the system. Corporate domain security policies and the Windows Integrated Security feature of Vijeo Citect is the recommended way to implement this.

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

Password aging must be used.

(c) Following loss management procedures to electronically de-authorize 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.

It is the customer's responsibility to ensure secure handling and control of usernames and identification codes. The use of Windows Integrated Security with Vijeo Citect is the recommended solution for this. The system has to be developed flexible enough to disable or lock out lost, stolen or compromised accounts by a user with proper rights, and add new permanent replacement with the proper controls in place of the lost account.

(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

Unsuccessful logins should be monitored and appropriate steps should be in place to alert management.

The Windows Integrated Security feature available in Vijeo Citect can be used to summarize login failures and lock or disable the user account automatically after the preset failed login limits reached.
Successful login shall reset the login failure counter.
Locked or disabled user accounts shall be possible to re-enable based on the decision of management by system administrator.

(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

It is the customer's responsibility to implement procedures to ensure devices are functioning properly and that they have not been altered.

Security

FDA

Security

FDA