Food and Drug Administration's (FDA's) application of part 11 of Title 21 of the Code of Federal Regulations; Electronic Records; Electronic Signatures (FDA 21 CFR Part 11)

Introduction

FDA 21 CFR Part 11 is a regulation established in 1997 that provide a framework for using electronic records and signatures in place of paper records and handwritten signatures, while maintaining the same level of reliability, authenticity, and integrity as paper records.

The Code of Federal Regulations (CFR) comprises the consolidated and enduring set of rules and regulations issued by the executive departments and agencies of the United States federal government, as published in the Federal Register. The CFR covers a broad range of topics and is organized into 50 titles. Title 21 of the CFR specifically pertains to Food and Drugs.

The Food and Drug Administration (FDA), Drug Enforcement Administration (DEA), and Office of National Drug Control Policy (ONDCP) are three key regulatory agencies responsible for enforcing Title 21 of the Code of Federal Regulations in the United States. Title 21 governs various aspects of food and drug safety and is composed of three chapters. Chapter 1 pertains to the FDA, Chapter 2 to the DEA, and Chapter 3 to the ONDCP.

Chapter 1 has 99 parts and Part 11 deals mainly with electronic records and electronic signatures.

The key requirements of the FDA 21 CFR Part 11 are:

1. Validation: Electronic records and signatures must be validated to ensure that they are reliable, accurate, and secure.
2. Security: Electronic records must be protected from unauthorized access, modification, or deletion.
3. Audit trails: Electronic records must be accompanied by an audit trail that documents all actions taken on the record.
4. Electronic signatures: Electronic signatures must be unique to the individual, securely managed, and linked to the corresponding electronic record.
5. Retention and retrieval: Electronic records must be retained and retrievable throughout their retention period.

This document provides information about features available in ADISRA SmartView that enable application engineers to design Human Machine Interface (HMI)/Supervisory Control and Data Acquisition (SCADA) applications in accordance with the FDA 21 CFR Part 11 regulations.

While the software (SCADA/HMI) cannot assert its own compliance with FDA 21 CFR Part 11, it is designed to furnish users with the essential tools needed to develop an application that adheres to the FDA 21 CFR Part 11 requirements.

For more information on these features, please refer to the Technical Reference (Help) manual of the product or the FDA 21 CFR Part 11 video in our video library (https://adisra.com/video-library/).

Electronic Signature

Effective management of user accounts and credentials is crucial for complying with the requirements of Part 11. ADISRA SmartView offers a range of options for managing users and roles, making it adaptable to different corporate environments and use cases. These options include internal management (within ADISRA SmartView), external management (using an external database or enterprise identity provider), and Active Directory (enterprise-managed).

Internal Management

ADISRA SmartView features a robust and all-inclusive security system that enables application engineers to establish access and control policies for their projects, based on user authentication.

ADISRA SmartView provides features.

1. User Authentication: ADISRA SmartView Security System has user authentication mechanisms, such as username and password, to control access to the system. User accounts should be unique and tied to specific individuals with assigned roles and responsibilities.
2. User Access Control: ADISRA SmartView offers granular access control, restricting users to perform only the actions necessary for their roles. This helps maintain data integrity and prevents unauthorized access or modifications.
3. Electronic Signatures (also referred to as e-signatures): ADISRA SmartView supports electronic signatures to demonstrate that certain actions or changes were performed by authorized individuals. E-signatures are linked to specific users and include the date and time of the action.
4. Audit Trail: ADISRA SmartView provides electronic audit trail that records all significant events, such as system changes, configuration modifications, and critical data alterations. The audit trail is secure, time-stamped, and accessible only to authorized personnel.
5. Data Integrity: ADISRA SmartView ensures the integrity of electronic records, preventing unauthorized modifications and ensuring data accuracy throughout its lifecycle.
6. Encryption: ADISRA SmartView provides encryption to protect sensitive data in transit and at rest within the ADISRA SmartView environment.

External Management (using an external database)

ADISRA SmartView provides FDA 21 CFR Part 11 compliance features, as mentioned earlier. Additionally, it offers database connectivity, enabling the use of FDA 21 CFR Part 11 compliance features within the database. Depending on the chosen database, external databases can ensure the authenticity, integrity, and security of electronic records and signatures through the following capabilities.

1. Secure Electronic Record Storage: The database acts as a safe repository for electronic records generated by ADISRA SmartView.

2. Data Integrity Measures: The database employs measures to maintain data accuracy, completeness, and reliability.
3. Audit Trail Creation: An electronic audit trail is established, tracking all significant activities related to electronic record-keeping.
4. User Authentication and Electronic Signatures: The database supports user authentication and electronic signatures, ensuring actions are securely linked to authorized users.
5. Access Controls: Administrators can define specific privileges for individual users or groups, enabling granular access control.
6. Database Backup and Recovery: Mechanisms for data backup and recovery prevent data loss in case of system failures or incidents.
7. Record Retention and Archiving: The database facilitates record retention for the required duration and enables inspection and review.
8. Validation and Change Controls: Changes to the database, like schema modifications, are documented and validated.
9. Data Retrieval and Reporting: Authorized personnel can access and review electronic records for inspections, audits, and regulatory submissions.
10. Data Encryption and Transmission Security: Sensitive data is protected at rest and during transmission through encryption.

Active Directory

ADISRA SmartView, when integrated with Active Directory for FDA 21 CFR Part 11 compliance, strengthens security measures, authentication, and access control for electronic records and signatures.

Here are some key aspects to consider for ADISRA SmartView with Active Directory integration:

1. User Authentication and Authorization: Active Directory can serve as the central authentication system for ADISRA SmartView. It enables user logins using their Active Directory credentials, ensuring that only authorized personnel can access the system.
2. Electronic Signatures: Active Directory integration can facilitate electronic signatures in ADISRA SmartView. User identities from Active Directory can be linked to their electronic signatures, which are then used by ADISRA SmartView for example, to indicate approvals and authorizations for various actions, such as starting or stopping processes, changing setpoints, adding new devices, changing data tags, or adjusting operational parameters.
3. Role-Based Access Control (RBAC): Active Directory allows for the implementation of RBAC within ADISRA SmartView application. Different user roles can be defined in Active Directory, and ADISRA SmartView can use these roles to enforce granular access controls and limit user actions based on their assigned privileges.
4. User Management and Audit Trail: Active Directory provides tools to manage user accounts, password policies, and account lockout settings. It can also maintain an audit trail of user authentication and changes to user accounts, enhancing security and traceability.

5. Data Integrity and Security: Active Directory incorporates essential security features like password policies and account lockouts, providing protection for user accounts and thwarting unauthorized access. This ensures the integrity and security of electronic records within ADISRA SmartView. When an employee departs from the company, Active Directory, functioning as a centralized user management system, manages the process in a controlled and secure manner, particularly in applications like ADISRA SmartView that utilize Active Directory for access control.
6. Data Backup and Recovery: Ensuring proper implementation of data backup and recovery procedures for Active Directory is essential, given its critical role in authentication and user management.

ADISRA SmartView provides a comprehensive set of options for managing users and roles, allowing organizations to tailor their approach to various corporate environments and use cases. Whether through internal management within ADISRA SmartView, external management utilizing an external database or enterprise identity provider, or integration with Active Directory for enterprise-wide management, ADISRA SmartView offers flexibility and adaptability to meet the diverse needs of regulated industries.

Electronic Records (Alarms, Event Logger, and Reports)

In the context of an HMI/SCADA package like ADISRA SmartView, electronic records, as defined by FDA 21 CFR Part 11, encompass any data, information, or documentation that is created, gathered, stored, and managed in electronic format within the system. These electronic records comprise a diverse range of data and documents critical for the operation, monitoring, and control of processes in FDA-regulated industries.

1. Alarms: ADISRA SmartView incorporates an alarm system that activates when specific pre-defined conditions or thresholds are met, signifying abnormal or potentially hazardous situations within the process. These alarms promptly notify operators and personnel, empowering them to respond promptly and take appropriate actions to address the identified issues. The alarm system enhances overall safety and process control, ensuring timely interventions to mitigate risks and maintain operational stability meeting documentation requirements of FDA 21 CFR Part 11.
2. Event Logger: In ADISRA SmartView, the event logger plays a role in capturing and recording significant events and activities that take place during the system's operation. These events encompass changes to process parameters, equipment status, operator interactions, system events, and other relevant occurrences. The event logger meticulously timestamps each event and securely stores it as an electronic record within the system. This meticulous process creates a comprehensive audit trail, ensuring the authenticity, integrity, and accountability of electronic records in compliance with regulatory standards.
3. Reports: Within ADISRA SmartView, reports play a vital role in offering valuable insights into process performance, historical trends, and operational data. These comprehensive reports encompass a wide range of information, such as data trends, batch records, event logs, alarms history, and other critical operational and compliance-related details. Through these reports, operators and stakeholders gain a clear understanding of system performance, enabling informed decision-making and proactive measures to optimize processes and maintain regulatory compliance.

FDA 21 CFR Part 11 establishes guidelines for utilizing electronic records and signatures in lieu of paper records, with a focus on maintaining reliability, authenticity, and integrity. ADISRA SmartView incorporates essential features to comply with these regulations, such as user authentication, access control, electronic signatures, and data integrity measures. In essence, ADISRA SmartView is designed to align with FDA 21 CFR Part 11 requirements, equipping users with the necessary tools to develop HMI/SCADA applications that meet regulatory standards in FDA-regulated industries.

For more information on ADISRA SmartView, please visit our website at www.adisra.com or send email to infor@adisra.com.