



APOGEE[®] Compliance Solution for FDA-Regulated Facilities

Technological Elements for 21 CFR Part 11 Compliance

Building Technologies

SIEMENS

Insight®

Firmware

Infocenter®

Network

21 CFR Part 11 Requirement

Data Integrity

The integrity of the APOGEE system data is validated to ensure that the APOGEE system meets all Functional Specification and Design Specification requirements. Siemens has established standard IQ/OQ protocols to validate the APOGEE system and to maintain the APOGEE system operations at a "Validated Level" throughout the lifetime of the APOGEE system.

Establish Procedures

The customer has to develop 'internal' Standard Operating Procedures (SOPs) for the proper use and operation of the building automation system. Siemens recommends that the following SOPs be developed for a customer site: System Operating Procedures, Backup Procedures, Change Control/ Upgrade Procedures, Hardware Maintenance Procedures, Calibration Procedures, Software Maintenance Procedures, eSystem Security Procedures, Training Procedures, Electronic Records/Data Management Procedures, Incident Management Procedures and Disaster Recovery Procedures.

Control Documents

The Customer needs to have the required documentation available and protected. Revision and change control procedures should be in place for all the required documentation. The list of the required documentation includes, but is not limited to: User Requirements, Functional Design Specification, Operations and Maintenance Manuals, Training Records, Calibration Records, System Drawings, Complete Protocol Documents, System Acceptance and Sign-off and Maintenance Records.

Protection of Records

The Insight workstation retains complete copies of system records in both human-readable and electronic form, available for inspection, review and copying.

It is recommended that power be sourced from an uninterrupted power supply (UPS) and the UPS is sourced from an emergency power grid. This practice eliminates loss of data due to power blackouts, brownouts, surges or dips.

Robust server designs are installed with built-in redundancy to protect data stored on the server hard disk. SOPs are used to regularly backup critical electronic records.

Access to the system is integrated with Windows® security. Users DO NOT have to manage a unique set of usernames and passwords. Using each individual's Windows account name and password, the system can detect user access and can grant them access to only those functions they are authorized to use. This access control is used to determine what functions a user can use, what they can view, print or otherwise have access to.

Password security and physical security must be enabled at the field panels. It is recommended that the BLN system access is limited to Read-Only access by default.

It is recommended that power be sourced from an uninterrupted power supply (UPS) and the UPS is sourced from an emergency power grid. This practice eliminates loss of data due to power blackouts, brownouts, surges or dips.

It is recommended that power be sourced from an uninterrupted power supply (UPS) and the UPS is sourced from an emergency power grid. This practice eliminates loss of data due to power blackouts, brownouts, surges or dips.

Robust server designs are installed with built-in redundancy to protect data stored on the server hard disk. SOPs are used to regularly backup critical electronic records.

Access to the system is integrated with Windows security. Users DO NOT have to manage a unique set of usernames and passwords. Using each individual's Windows account name and password, the system can detect user access and can grant them access to only those functions they are authorized to use. This access control is used to determine what functions a user can use, what they can view, print, or otherwise have access to.

An Atomic Radio Clock with remote antenna synchronizes system server time. Access to the server clock is restricted by physical and software security measures.

All components with time functions in the APOGEE system are synchronized to the system server four times daily by using Microsoft® Windows Scheduled Task function and scheduling the SyncTime.exe file.

Redundancy of network components is recommended to ensure protection of records.

System Security

Systems that incorporate the APOGEE GO® for Insight or the Insight Terminal Services Option must incorporate additional security authentication measures, encryption mechanisms, firewall, and/or SSL (secure socket layer) type technologies into building automation design.

Access to the system is integrated with Windows® security. Users DO NOT have to manage a unique set of usernames and passwords. Using each individual's Windows account name and password, the system can detect user access and can grant them access to only those functions they are authorized to use.

Password security and physical security must be enabled at the field panels. It is recommended that the BLN system access is limited to Read-Only access by default.

TEC with Secure Mode prevents unauthorized users from making changes to the TEC through the MMI port. It is supported on Insight 3.7 and higher.

Access to the system is integrated with Windows security. Users DO NOT have to manage a unique set of usernames and passwords. Using each individual's Windows account name and password, the system can detect user access and can grant them access to only those functions they are authorized to use.

Access rights to system records, reports, report templates, and client applications are all controlled using Windows integrated security. Windows integrated security is designed and configured properly to limit system access through a SOP.

Trend Data

The ability to change Trend Definitions is restricted by Insight Access and Privileges. It is recommended that access capability be limited to a single individual and his/her supervisor.

It is necessary to collect Trend Data from field panels as often as possible to mitigate and/or significantly reduce possible loss of data stored in panel RAM. This design consideration must be considered in detail in specifications and validated.

The InfoCenter Suite Solution will acquire trend data records as they are created, lock them down in a secure database, provide the ability to retain them for a user definable and/or indefinite time and provide modern reporting functionality.

The InfoCenter System Activity Viewer manages system activity/operator transaction records.

Alarms

The ability to change Alarm parameters in Point Definitions is restricted by Insight Access and Privileges. It is recommended that access capability be limited to a single individual and his/her supervisor.

System alarm transaction records are managed by the Insight System Activity Log application.

Implementing the Alarm Issue Management Option for Insight allows the life cycle of an alarm to be managed in a paperless manner. It ensures that each step of the alarm process is documented to provide information as to what corrective action was taken, action assigned (person assigned and protocol to follow), response, and resolution of alarm.

Alarm configuration is part of the Point Definition database.

The InfoCenter Suite Solution will acquire alarm records as they are created, lock them down in a secure database, provide the ability to retain them for a user definable and/or indefinite time and provide modern reporting functionality.

System Activity

The ability to access System Activity Log is restricted by Insight Access and Privileges. It is recommended that access capability be limited to a single individual and his/her supervisor.

At the Field Panel, local system access should be restricted to a single individual and his/her supervisor. Operator access to field panel applications is limited by BLN Account access and privileges assigned under the Insight User Account application. Operator actions are logged by the Insight System Activity Log application.

The InfoCenter Suite Solution will acquire system activity records as they are created, lock them down in a secure database, provide the ability to retain them for a user definable and/or indefinite time and provide modern reporting functionality.

Point Definitions

The ability to change Point Definitions is restricted by Insight Access and Privileges. It is recommended that access capability be limited to a single individual and his/her supervisor.

At the Field Panel, point definitions such as: point names, alarm limits, operator messages, slope/intercept, default values are stored in EEPROM and protected from data loss during power failures by battery within the field panel.

The InfoCenter Suite will acquire operator transaction records as they are created, lock them down in a secure database, provide the ability to retain them for a user definable and/or indefinite time and provide modern reporting functionality.

PPCL

The ability to change PPCL is restricted by Insight Access and Privileges. It is recommended that access capability be limited to a single individual and his/her supervisor.

At the Field Panel, PPCL programs are stored in the EEPROM memory and protected from data loss by battery within the field panel.

Audit Trails

Field Panel Firmware Release 2.6, 2.7, and 2.8 and Insight Version 3.5.1 and higher provide an audit trail of any changes made to PPCL, Point Definitions and other critical point classification information. The Insight System Activity Log application captures and documents changes to the APOGEE system operations.

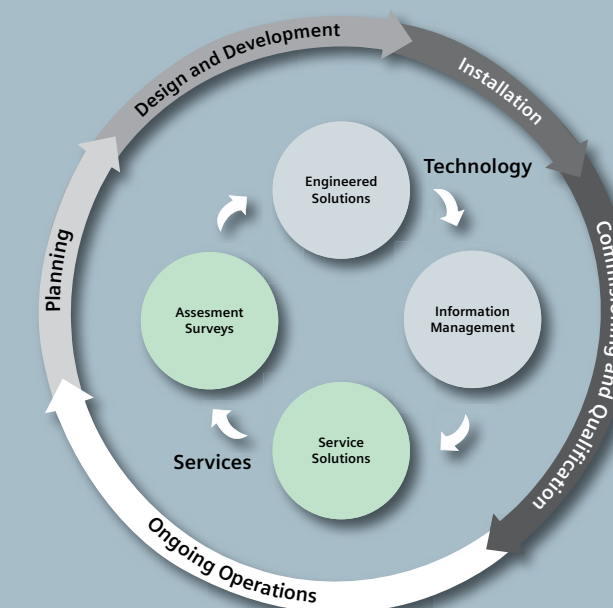
The Compliance Support Option allows detailed tracking of modifications and deletions of supervised objects. With this option, you can track which property of an object was changed, its value before and after the change, why the change was made, who authorized the change, and where the change was made from. This protects the system from inadvertent changes.

A direct data transfer exists for trend, alarm, and other data interchange/interface between Insight Version 3.5.1 and higher and InfoCenter Version 1.4 and higher.

Electronic Signatures

The digital signatures feature is based on InfoCenter Suite's PDF-based report output option and uses a signature handler plug-in to Adobe® Acrobat®.

A complete facility life cycle solution

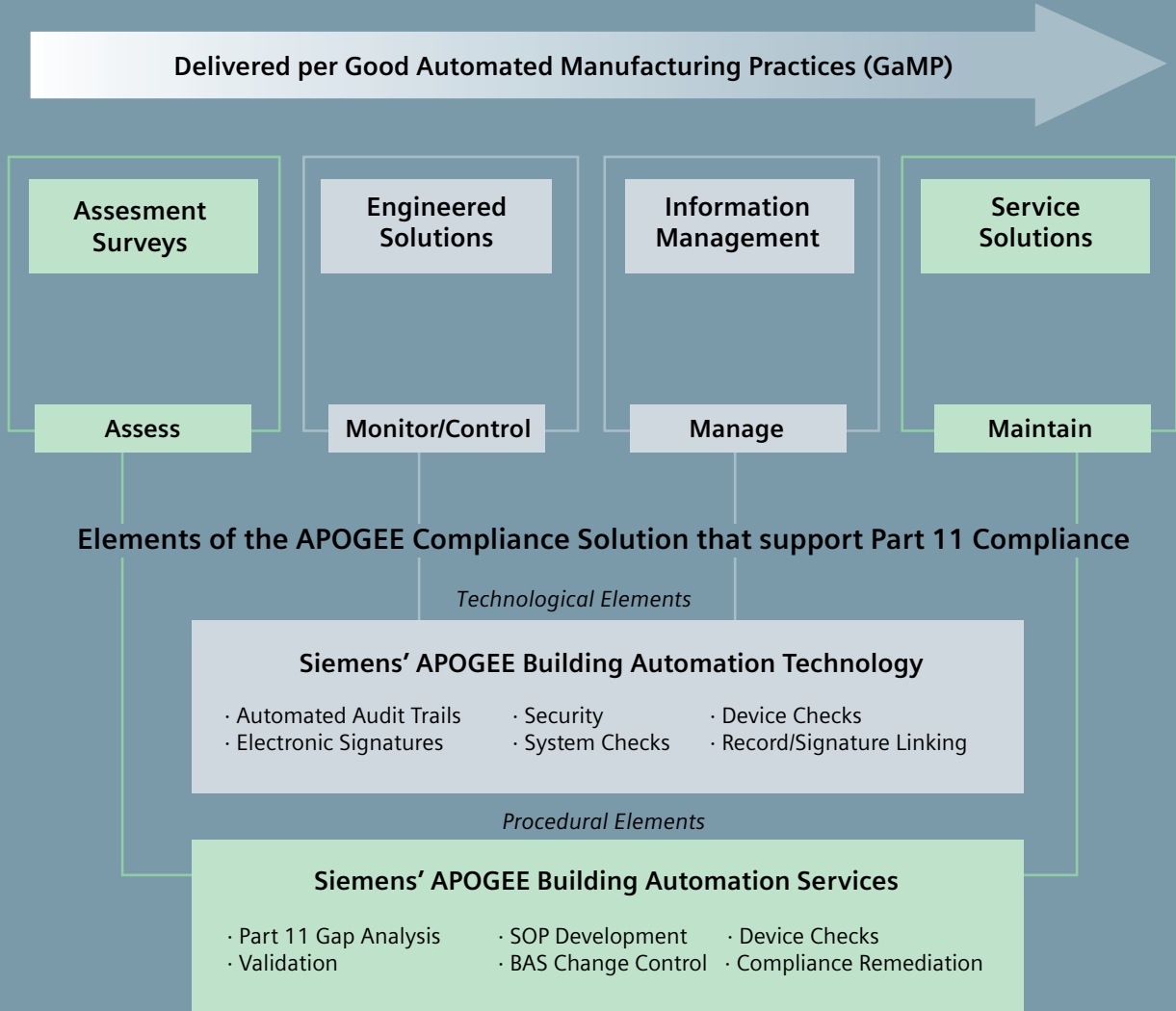


The APOGEE® Compliance Solution for FDA-Regulated Facilities

Technological Elements for 21 CFR Part 11 Compliance

This solution set matrix offers a brief overview of how the APOGEE Compliance Solution for FDA-Regulated Facilities meets the technological requirements of Rule 21 CFR Part 11. Electronic systems for FDA regulatory compliance must address various issues such as record protection, data trending, alarming, audit trails, system

security and others. Here we briefly review how the various components of our solution address these issues. In addition, suggestions are made regarding other requirements that must be met such as power management, disaster recovery or other necessary functions and procedures.



Siemens Building Technologies, Inc.
1000 Deerfield Parkway
Buffalo Grove, IL 60089
Tel: (847) 215-1000
Fax: (847) 215-1093

APOGEE, APOGEE GO,
Insight, and InfoCenter Suite
are registered trademarks of
Siemens Building Technologies, Inc.
Microsoft and Windows are registered
trademarks of Microsoft Corporation.
Adobe and Acrobat are registered
trademarks of Adobe Systems Incorporated.

© 2008 by Siemens Building
Technologies, Inc. All rights reserved.
Country of origin: US. 150-610P10 (08/08)

www.usa.siemens.com/buildingtechnologies