



Automation Change Management *Proficiency™ Change Management*

Guide Form Specification

GFT-512

February 2009

Automation Change Management – Guideform Specification

1	Overview	4
1.1	Purpose	4
1.2	Key Objectives and Benefits	4
1.3	Definitions	4
1.4	Industry Standards	5
2	Technical Requirements	6
2.1	System Architecture	6
2.2	System Requirements	6
2.3	Licensing	6
3	Software Requirements	8
3.1	Client/Server System	8
3.2	Security	8
3.3	Version Management	9
3.4	Electronic Signature	9
3.5	Audit Trails	10
3.6	Administration	10
3.7	User Interface	11
3.8	Scheduled Compare and Backup	11
3.9	Device and Product Support	11
3.10	Documentation	14
3.11	Software Connectivity	14
4	Service and Support	15
4.1	Training	15
4.2	Installation Services	15
4.3	Testing and Validation	15
4.4	Software Warranty	15

Automation Change Management - Guideform Specification

5	Vendor Requirements	17
5.1	Development Life Cycle	17
5.2	ISO 9001 certified	17
5.3	Preferred Vendor / Manufacturer	17
6	Appendix	18
6.1	Glossary	18

1 Overview

1.1 Purpose

The purpose of this paper is to capture requirements for an Automation Change Management System for Plant Operations, IT and operators. The objective is to outline high-level user requirements for the shop floor level management of control system software like PLCs, HMI, SCADA, and other programmable devices.

1.2 Key Objectives and Benefits

The key objective to implementing an Automation Management System is to reduce downtime, re-engineering, and equipment loss due to misplaced databases or other preventable errors.

The key benefit of an Automation Management System would be to electronically manage the shop floor software that runs plant devices. The Automation Management System will be responsible for the management, storage and version control of PLC, SCADA, and other device configuration and program required for the control systems in the plant. It will provide a secure repository for these configurations and aid in the disaster recovery of any system.

Key objectives of Automation Management System include are:

- To aid in the disaster recovery of control systems in the plant
- Provide a secure environment for program storage.
- To provide a centralized, version-controlled repository for PLC, HMI, SCADA, and other device programs as well as miscellaneous documents
- To enable offline – online comparisons of PLC configurations to ensure program integrity
- Provide reliable shop floor software storage.
- Provide traceability for shop floor software changes.
- Provide a consistent single interface to access and modify these device programs and documents.
- Enhance compliance with FDA CFR 21 Part 11
- Enhance cGMP compliance
- Enhance compliance with NERC

1.3 Definitions

- HMI: Human Machine Interface. Used to provide a graphic representation of data from a process and to accept user commands to be fed back to the process.
- Ethernet: A very high performance local area network standard providing the two lower levels of the ISO/OSI seven layer reference model, the physical layer and the data link layer.
- TCP/IP: a protocol widely used across Ethernet networks for connecting computers and programmable controllers.
- Web Browser: A client application that provides a user interface via the World Wide Web. Netscape and Microsoft Internet Explorer are two popular examples.

Automation Change Management – Guideform Specification

- Thin Client: In client/server applications, a client designed to be especially small so that the bulk of the data processing occurs on the server. The term *thin client* refers to a client designed to be as small as possible.
- Data Concentrator: A physical device that translates analog and digital information from attached I/O devices to a protocol that can be used with an HMI.
- Communications Protocol: A formal set of conventions governing the control of Inputs and Outputs between the two communicating processes.
- Network: An interconnected group of nodes, a series of devices, nodes or stations connected by communications channels.
- Operating System: A program that controls the entire overall operation of the computer system hardware / software.

1.4 Industry Standards

The US FDA requirements for cGMP include the following key requirements:

- 21 CFR Part 11 - electronic signatures and records. 21 CFR Part 11 establishes the criteria under which electronic records and electronic signatures will be considered equivalent to paper records and hand-written signatures executed on paper. The rule applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in FDA regulations.
- 21 CFR Part 210 - current Good Manufacturing Practice in manufacturing, processing, packing, or holding of drugs.
- 21 CFR Part 211 - current Good Manufacturing Practice for finished pharmaceuticals.

2 Technical Requirements

2.1 System Architecture

Overview of how pieces fit together.

Hardware and Software Architecture

2.2 System Requirements

2.2.1 Operating System - Server

The operating system shall be Microsoft Windows XP, Windows 2003 Server, Windows 2009 Server or Windows Vista. The software shall exhibit strong compliance with Microsoft's Windows Open Systems Architecture (WOSA) standards, such as in its use of dialog boxes and menus. The system must support running as a service under Windows, making it independent of the user login limitations.

2.2.2 Operating System – Client

The operating system shall be Windows XP Professional, Windows 2003, Windows 2008, or Windows Vista.

2.2.3 Networking

The system shall be capable of supporting the following network configurations:

Network Adapters:

Ethernet

Network Protocols:

NetBIOS

TCP/IP

2.3 Licensing

2.3.1 Server Based Licensing

Licensing should be Server based and not require individual client licensing

2.3.2 Scalability

Licensing should be based on number of users, and easily allow for expansion of the system.

2.3.3 Concurrent Licensing

Licensing of the clients should be based on concurrent users, such that a user is counted only when active.

Automation Change Management – Guideform Specification

2.3.4 License Recovery

Licensing system should be designed to allow for graceful recovery from server or client rebuild (in the event of loss of system or hard-drive).

3 Software Requirements

3.1 Client/Server System

- 3.1.1 The system shall include a dedicated Configuration Manager PC or sever that is used to administer the Automation Management functions and stores the managed configurations.
- 3.1.2 Server administration needs to be accessible from any client.
- 3.1.3 System needs to allow adding of projects/configurations from any client
- 3.1.4 The system shall allow for working disconnected from the server. While disconnected, Security and Audit trailing needs to be maintained.
- 3.1.5 The system shall provide an option for a ‘thin’ end user client, where the client can be hosted on web server and not require local installation, and where end user refers to the common operations a user wishing to view or edit the files being managed.

3.2 Security

- 3.2.1 The security system needs to be able to synchronize with existing network Windows domain security. The domain server will authenticate passwords. Use of the domain security will allow enforcement of the 21 CFR Part 11 guidelines, which include password expiration, enforcement of a unique user ID, etc.
- 3.2.2 Access to administrative functions needs to be limited to those with Administrative privileges.
- 3.2.3 Access to all parts of the system needs to be limited to only configured users.
- 3.2.4 Access to the security system needs to be permission based, must prevent two administrators from changing the security settings at the same time.
- 3.2.5 Provide multi-level security with Users and Groups. Groups need to be definable at the site and can by job function, location, or using other criteria.
- 3.2.6 Permissions assigned to groups will enforce the functionality available for those users.
- 3.2.7 User Groups – system should support various groupings of users that can have assigned roles and capabilities specific to the configuration management system.
- 3.2.8 User can belong to one or more groups. The system should enforce operations based on the highest level of permission the groups will provide that user.
- 3.2.9 The system shall provide for a unique combination of two distinct identification components (username and encrypted password) for electronic signatures typed in or captured by another input means.
- 3.2.10 In the event of reaching the maximum number of failed login attempts, the system shall block the user account and notify the administrator by means of a message.
- 3.2.11 The system shall log a user out or lock the workstation after a specified inactivity time such that the logged in user or an administrator can unlock it.

3.3 Version Management

- 3.3.1 Access to a project will be limited by the privileges of the user as configured by the security
- 3.3.2 The version control system shall allow for an unlimited number of versions.
- 3.3.3 Automatic Version Numbering: The version control system shall automatically increment version numbers as changes are checked into the system.
- 3.3.4 The system shall provide an interface for reporting on revision history of a specific program.
- 3.3.5 It should not be possible to delete historical versions from the system through the user interface.
- 3.3.6 The system shall allow the ability to revert to a previous version of a file or project without deleting the newer versions in the system.
- 3.3.7 To make modifications to a project or configuration file, the system needs to require a Check out process. This check out process needs to be able to limit one person to have check out status at a given time.
- 3.3.8 While one user has a project checked out, other users shall have the ability to retrieve a read only copy of the project file(s).
- 3.3.9 The ability to designate a master version shall be available. The master version should be permission based such that only those with proper authority can designate it.
- 3.3.10 Version numbers shall not be editable
- 3.3.11 The system shall have the facility to add version comments as each version is saved.
- 3.3.12 It needs to be possible to retrieve an older version of a document in a read only format.

3.4 Electronic Signature

- 3.4.1 The system should be able to handle the addition of electronic signatures to authorize changes or deletion of projects.
- 3.4.2 The number of signatures and the verifications shall be configurable for each project.
- 3.4.3 Changes to the configuration of the Electronic Signature system shall be indicated in the Audit Trail.
- 3.4.4 Electronic signatures shall include user verification and one or two signatures per any project or configuration change.
- 3.4.5 The user submitting the changes must be verified prior to seeking the approvals.
- 3.4.6 The user submitting the changes must be forced to enter a change comment to describe the changes.
- 3.4.7 Users should have the ability to enter comments at time of signing and the system should allow for comments to be selected from a predefined list or entered in a free from text box.
- 3.4.8 Users from pre-defined authorization groups shall perform authorization.
- 3.4.9 The Electronic Signature system shall allow external systems to be used to gather signature information and interface back to the change control system through an API.

Automation Change Management – Guideform Specification

- 3.4.10 21 CFR part 11 guidelines shall be enforced during the signature process. The user submitting the change cannot approve the changes, and when 2 signatures are required, the 2 users must be unique.
- 3.4.11 Change record in the Audit Trail must provide the user initiating the change, and the one or two authorizing signatures with comments.

3.5 Audit Trails

- 3.5.1 The Audit Trail database shall be configurable for one of Access, SQL Server, or Oracle.
- 3.5.2 The Audit trail database needs to be able to be secured if using SQL Server or Oracle, such that it cannot easily be tampered with.
- 3.5.3 The system shall record user and administrative actions in the system.
- 3.5.4 Changes made by the user to projects (i.e. Check in, Check out, Open, etc.) shall be logged in the audit trail database.
- 3.5.5 The database shall store as a minimum:
 - Date and Time in UTC format
 - User ID and Full user name
 - Location or PC Name
 - The action that was performed (Check in, Check out, etc)
 - User commentIf electronic signature is enabled:
 - User verification and comment
 - Authorization user with comment
 - Second Authorization user with comment
- 3.5.6 Audit Reports - Audit reports need to be available in a human readable format, either through a built in reporting tool, or 3rd party tools. The delivery of the reports shall be in a format, such that they cannot be tampered with.
- 3.5.7 The actions that trigger an audit entry should be configurable based on the product type and general actions such as login/logout.
- 3.5.8 Changes to the audit configuration shall be recorded be the audit trail itself, such that if an audit is turned off, it is traceable to the individual that made the change.
- 3.5.9 The system shall have the ability to trigger email notifications based on the audit events, such as check in operations, scheduled compare results. It should allow for creation of rules based on plant area, user, project name.

3.6 Administration

- 3.6.1 Administration functions shall be available only to those users belonging to the administrator groups, or to those granted permission for the specific administrative function.

Automation Change Management – Guideform Specification

3.6.2 Administration of the system needs to be possible from any thick client. The user must have appropriate permissions to access these functions.

3.6.3 Administrator group shall have access to all functions in the system.

3.7 User Interface

3.7.1 Interfacing with the system should be available by a client interface using a WEB browser.

3.7.2 System shall require a standard explorer style interface to access projects.

3.8 Scheduled Compare and Backup

3.8.1 The scheduling system shall allow for both centralized server based scheduling of tasks, or have the ability to assign tasks to remote scheduling stations.

3.8.2 The scheduling system shall allow for scheduling of tasks on an hourly, daily, weekly, monthly, or manual basis.

3.8.3 The system shall allow for the ability to automatically compare the running code in a controller or a set of files to the appropriate version on the server.

3.8.3.1 The system shall allow the ability to select whether to compare to the latest version or the master version of the project files.

3.8.4 The system shall have the ability to notify specified users of the results of the scheduled compare results.

3.8.5 The scheduling system shall allow for end-user defined tasks. Custom tasks will developed using a common language such as Visual Basic.

3.8.6 The system shall allow for the ability to have the system automatically backup the version of the appropriate files if differences are detected wherever possible. If a backup is created, a new version shall be created on the server

3.8.7 The system shall provide support for a variety of popular devices as defined in the device and product support section.

3.9 Device and Product Support

3.9.1 The system will need to provide support for configurations for PLCs from multiple vendors. Project Management indicates the basic ability to provide Version Control, Audit Trailing, and Security access for the files managed by the system. Support will include:

3.9.1.1 GE Fanuc 90-30 and 90-70 Series PLCs

Support needs to available using LogicMaster., VersaPro, and Machine Edition Software. Support for these devices is to include

- Version Control
- Project management
- Manual and Automated comparison functions

3.9.1.2 GE Fanuc PAC Systems

Automation Change Management – Guideform Specification

Support for these devices is to be made available using Machine Edition Logic Developer PLC software. Support needs to include a minimum of:

- Version control and management of projects
- Detailed Security including limiting of online, offline changes, data changes, forcing and configuration changes.
- Manual and Automated comparison functions

3.9.1.3 GE Fanuc CNCs

The system shall have the ability to manage, compare, and backup GE Fanuc CNC controls. System needs to support backup and compare via the HSSB or Focas Ethernet. Models to be supported include 16C, 16i, 18C, 18i, 21C, and 21i.

3.9.1.4 GE Fanuc HMI/SCADA iFIX

The system shall support iFIX as both a complete project, or individual components. For the overall projects, the support shall include:

- Version Control
- Project management
- Manual and Automated comparison functions

With individual components:

- Client built into the Workspace
- Ability to version control picture files, tag database, configuration, security, recipes and other components that make up the application.
- Provide detailed audit history of components that are being modified
- Provide detailed comparison reports on the picture files and configuration

3.9.1.5 GE Fanuc HMI/SCADA CIMPLICITY

The system shall support CIMPLICITY as both a complete project, or individual components. For the overall projects, the support shall include:

- Version Control
- Project management
- Manual and Automated comparison functions detailing screen and point database modifications

With individual components:

- Client built into the Workbench
- Ability to version control screens, point database, configuration, security, recipes and other components that make up the application.
- Provide detailed audit history of components that are being modified
- Provide detailed comparison reports on the screens and configuration

3.9.1.6 Fanuc Robots

Automation Change Management – Guideform Specification

Support for Fanuc RJ3 robots shall be provided. This includes the ability to upload and compare the controls over Ethernet.

3.9.1.7 Rockwell SLC 500/Micrologix

Support for this device needs to available using RSlogix 500 Software. Support for these devices is to include

- Version Control
- Project management
- Manual and Automated comparison functions
- Data filtering on compares to regularly changing data doesn't cause exceptions
- Security settings to restrict online capability including Forcing, ladder and data changes
- Ability to synchronize PLC passwords

3.9.1.8 Rockwell PLC-5

Support for this device needs to available using RSlogix 5 Software. Support for these devices is to include

- Version Control
- Project management
- Manual and Automated comparison functions
- Data filtering on compares to regularly changing data doesn't cause exceptions
- Security settings to restrict online capability including Forcing, ladder and data changes
- Ability to synchronize PLC passwords

3.9.1.9 Rockwell Controllogix

Support for this device needs to available using RSlogix 5000 Software. Support for these devices is to include

- Version Control
- Project management
- Data filtering on compares to regularly changing data doesn't cause exceptions
- Security settings to restrict online capability including Forcing, ladder and data changes

3.9.1.10 Modicon 584/984

Support for this device needs to available using ProWorx Plus, ProWORX NxT, or ProWORX 32 Software. Support for these devices is to include

- Version Control
- Project management
- Manual and Automated comparison functions
- Detailed comparison reports

3.9.1.11 Modicon Quantum

Support for this device needs to be available using ProWORX NxT or Concept Software. Support for these devices is to include

- Version Control
- Project management
- Manual and Automated comparison functions
- Detailed comparison reports

3.9.1.12 Siemens S7

Support for this device needs to be available using Siemens Step 7 Software. Support for these devices is to include

- Version Control
- Project management
- Manual and Automated comparison functions

3.9.1.13 Siemens 840D CNC

Support for this device needs to be available using Siemens libraries and Step 7 Software. Support for these devices is to include

- Version Control
- Project management
- Manual and Automated comparison functions

3.9.1.14 ABB SC4 Robot

Support for this device needs to be available using a direct Robot interface. Support for these devices is to include

- Version Control
- Project management
- Manual and Automated comparison functions

3.10 Documentation

3.10.1 Product Documentation need to be available in online format within the product.

3.10.2 The online help system in the product needs to be context sensitive such that immediate help is available for the selected functionality.

3.10.3 Printed manuals need to be available as an option.

3.11 Software Connectivity

3.11.1 The system shall allow for the use of standard ODBC database connectivity to access the Audit Trail.

4 Service and Support

4.1 Training

- 4.1.1 The Site implementation team shall provide training and documentation on the maintenance and configuration of the system.
- 4.1.2 The Site implementation team shall provide training and documentation on the operation of the system.
- 4.1.3 Vendor needs to be able to provide both on-site and off-site training on administrating and using the product.
- 4.1.4 Product training shall be conducted by factory certified trainers.

4.2 Installation Services

- 4.2.1 The vendor shall have the ability to provide qualified consulting and installation services. These services need to be provided either by the vendor or via certified partners. Services include:

- Site Assessment
- Consultation
- Implementation
- Assistance and turnkey
- Validation services

- 4.2.2 Global Services

Vendor needs to be able to provide service and support the installations locally worldwide.

4.3 Testing and Validation

- 4.3.1 The supplier will develop a Site Acceptance Test (SAT) to be executed at the facility. The results of the SAT will be used as the basis of acceptance.
- 4.3.2 The vendor shall have the ability to assist in a formal validation process.

4.4 Software Warranty

- 4.4.1 Vendor shall provide the option to purchase support contract. This contract is to include:

- Phone support
- E-Support
- On-site
- 24 x 7 x 365

- 4.4.2 The vendor shall have a location on their web site where users can download software improvements, bug fixes, add-ons, components and so forth. The vendor shall provide a mechanism to install software improvements and bug fixes without the need for uninstalling or reinstalling the software application – only the changed components need to be replaced or upgraded.

Automation Change Management – Guideform Specification

- 4.4.3 The vendor shall also provide an easy mechanism for upgrading and installing software improvements and for allowing a user to quickly ascertain what improvements have been installed.

5 Vendor Requirements

5.1 Development Life Cycle

- 5.1.1 The vendor must have an established development life cycle that allows for traceability of features and functions throughout that life cycle.
- 5.1.2 The vendor must have a formal and documented set of quality assurance procedures that are applied to the engineering design, development, and documentation of the software. The presence of a formal quality assurance department shall be required.
- 5.1.3 The vendor must also demonstrate that its source code for the product is regularly archived both on-site and off-site in facilities suitable to withstand physical harm.
- 5.1.4 The vendor shall allow for on-site auditing of the development life cycle to ensure good practice.

5.2 ISO 9001 certified

- 5.2.1 The vendor must be able to demonstrate that it has established procedures.
- 5.2.2 Vendor needs to be certified under the ISO 9001-2001 guidelines.

5.3 Preferred Vendor / Manufacturer

- 5.3.1 Pre-evaluation has identified that Proficy™ Change Management product from GE Fanuc Automation as the preferred software solution. Any proposed solution must include at a minimum the functionality contained in the current commercially available version of Proficy™ Change Management.
- 5.3.2 Licensing will be provided to support XX simultaneous users and will include an annualized contract for Proficy™ GlobalCare Support.

6 Appendix

6.1 Glossary

Database (ANSI): Collection of data fundamental to a system.

Design Specification:

GAMP Forum: This is a complete definition of the equipment or system in sufficient detail to enable it to be built. This links to Installation Qualification which checks that the correct equipment or system is supplied, to the required standards and that it is installed correctly.

IEEE: The specification that documents the design of a system or system component to satisfy specified requirements.

Documentation (ANSI N45.2.10-1973): Any written or pictorial information describing, defining, specifying, reporting or certifying activities, requirements, procedures, or results.

Installation Qualification [IQ] (PMA CSVC): Documented verification that all key aspects of [software and] hardware installation adhere to appropriate codes and approved design intentions and that the recommendations of the manufacturer have been suitably considered.

Integration Testing (IEEE): An orderly progression of testing in which software elements, hardware elements, or both are combined and tested until the entire system has been integrated.

Interface (ANSI/IEEE): A shared boundary to interact or communicate with another system component.

Life Cycle Concept (PMA CSVC): An approach to computer system development that begins with identification of the user's requirements, continues through design, integration, qualification, user validation, control and maintenance, and ends only when commercial use of the system is discontinued.

Master: Master or Master Disk is the current validated copy of PLC code for any given device; this is the offline copy of what should be running in any processor.

Network:

ANSI/IEEE: An interconnected or interrelated group of nodes.

GAMP Forum: An interconnected communications facility. A Local Area network (LAN) is a high bandwidth (allowing a high data transfer rate) computer network operating over a small area such as an office or group of offices.

Operating System:

PMA CSVC: A set of programs provided with a computer that function as the interface between the hardware and the application programs.

ANSI/IEEE: Software that controls the execution of programs. An operating system may provide services, such as resource allocation, scheduling, input/output control, and data management.

Automation Change Management – Guideform Specification

Operational Qualification [OQ] (PMA CSVC): Documented verification that the equipment-related system or subsystem performs as intended throughout representative or anticipated operating ranges.

Performance Qualification [PQ]: Documented verification that the process and/or the total process-related system performs as intended throughout all anticipated operating ranges.

Procedure (PMA CSVC): A directive usually specifying how certain activities are to be accomplished.

Qualification Protocol: A prospective experimental plan that when executed is intended to produce documented evidence that a system or subsystem has been properly qualified.

Quality Assurance [QA] (ANSI/IEEE): A planned and systematic pattern of all actions necessary to provide adequate confidence that the item or product conforms to established technical requirements.

Requirement (ANSI/IEEE): A condition or capability that must be met or possessed by a system or system component to satisfy a contract, standard, specification, or other formally imposed document. The set of all requirements forms the basis for subsequent development of the system or system component.

Security (IEEE): The protection of computer hardware and software from accidental or malicious access, use, modification, destruction, or disclosure. Security also pertains to personnel, data, communications, and the physical protection of computer installations.

Software (PMA CSVC): A collection of programs, routines, and subroutines that controls the operation of a computer or a computerized system.

System: An assembly of units consisting of one or more microprocessors, associated hardware and software applications.

Testing (IEEE): The process of exercising or evaluating a system or system component by manual or automated means to verify that it satisfies specified requirements or to identify differences between expected and actual results.

User: The pharmaceutical customer or user organization contracting a supplier to provide a product. In the context of this document it is, therefore, not intended to apply only to individuals who use the system, and is synonymous with Pfizer.

Validation: "Establishing documented evidence, which provides a high degree of assurance that a specific process will consistently produce a product meeting its pre-determined specifications and quality attributes".
- FDA Guidelines on General Principles of Process Validation May 1987.

Validation Plan: A plan created by the customer to define validation activities, responsibilities and procedures.