
**Applying Wonderware in
21 CFR 11 Compliant Applications**



What is 21 CFR Part 11?

Manufacturers in industries regulated by the U.S. Food and Drug Administration (the “FDA”) are required to maintain and submit records associated with the products they manufacture. These records contain information about the product as well as hand written signatures of the individuals who executed the process and/or authorized the execution.

Historically, these records have been kept in paper format and submitted for review to the FDA upon request. As computer systems became readily accepted in the manufacturing environment, however, the storage of these records in electronic format was explored to see whether maintenance of these records in electronic format offered volume and cost benefits over the paper equivalent.

Early on, these studies raised questions about utilizing electronic media for storage of this information. Without the proper checks and balances in place, it could be possible to corrupt a record without maintaining the original data or being able to discern that the data had been modified. Additionally, the handwritten signatures that were used to authorize and execute the production were legally binding to the owners of the signatures. There was no equivalent for signatures executed electronically.

Following these studies, the FDA issued the 21 CFR Part 11 regulations on electronic signatures and electronic records in 1997, to establish the criteria under which electronic records and signatures would be considered equivalent to paper records and hand written signatures in FDA regulated industries.

The 21 CFR Part 11 regulation was in part intended to ensure that whenever manufacturers replaced traditional paper records with electronic records, they implemented the replacement systems in a manner that was equivalent to the paper based systems they were replacing. The regulation only applies where the records being maintained must be submitted for review to the FDA.

Applying Wonderware in 21 CFR 11 Compliant Applications

Where relevant, Wonderware applications and tools incorporate features and functionality intended to help regulated industries achieve and maintain compliance with 21 CFR Part 11 while minimizing life cycle costs. That being said, it is important to note that Wonderware products do not generally fall under the jurisdiction of the FDA and that accordingly, while Wonderware products may be used to build user specific applications which are in turn used in regulated manufacturing processes, it is ultimately these end-user applications and not the Wonderware products that must comply with 21 CFR Part 11.

The purpose of this white paper is to briefly explain what the Food & Drug Administration’s “Title 21 - Code of Federal Regulations - Part 11” is; to define which Wonderware FactorySuite components are deployable in human-machine interface (“HMI”) and supervisory control and data acquisition (“SCADA”) applications under 21 CFR Part 11; to clarify the detailed FDA definitions contained in the regulation as well as how Wonderware’s software solutions respond to these requirements; and to identify Wonderware’s continued commitment to a software development strategy that reduces the cost of building and supporting 21 CFR Part 11 applications.

Outlining the “Focus” Application and Terms

Wonderware offers a wide variety of software products in its FactorySuite of automation software. The HMI/SCADA and database components usable in FDA validated applications will be referred in this document as the “focus” application. Wonderware is continually working toward reducing the amount of engineering effort required to implement 21 CFR Part 11 compliant applications, the following FactorySuite components will be reviewed as the base application for the focus of this document:

- Visualization and Scripting – InTouch® 7.11
- Alarms – InTouch® 7.11
- Historical Data – InSQL™ 7.1

In addition, it will be assumed for this document that these component products will only be used in “closed” systems. As defined in the FDA regulation, a closed system refers to 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 is in contrast to the FDA definition of “open” systems, which refer to 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.

Since the 21 CFR Part 11 regulation is so complex and detailed, table lists will be used wherever possible to clarify the definitions found in the regulation text. Table 1 below covers definitions for biometrics, digital signatures, electronic records and so forth.

Table 1

Definition	Comment
Biometrics means 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.	An example of a biometric would be the use of a retinal eye scan to verify the identity of a user.
Digital signature means 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.	Digital signatures are required for use with open systems and are outside of the scope of this document.
Electronic record means 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.	Examples of typical electronic signatures in the focus application would be data history, alarms and events.
Electronic signature means 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.	An electronic signature in the focus application would be the execution of entering both the username and password.
Electronic signature means 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.	An electronic signature in the focus application would be the execution of entering both the username and password.
Handwritten signature means 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.	Handwritten signatures are the traditional format that paper systems use to record an action or authorization.

Configuration Issues

When configuring any software application there are several options that will need to be invoked by the user as well as some practices that should be followed. Each application is different and must be analyzed individually as to the level of compliance with 21 CFR Part 11. The products used do not automatically indicate the level of compliance that is achieved. The implementation of those products is what will be tested. The regulation is intended to cover all pertinent functionality that could reside in an application. However, individual applications may not utilize all of the functionality described in the regulation and therefore will not have to comply with all portions of the regulation. This document describes a focus application that will need to comply with all sections of the regulation. In other applications, alternate methods may be employed that cover the specific requirements of that application.

The Security system built into Windows® NT® covers a large number of the security requirements found in the regulation. In order to utilize the Windows NT security system in InTouch, the InTouch Extensibility Toolkit must be utilized to write a script function that will authenticate InTouch log-in attempts based on Windows NT Domain User account information. This will require that the operating system of the workstation be either Windows NT or Windows 2000. (As part of Wonderware's commitment to lowering engineering cost of applications, this NT authentication functionality will be incorporated as a natural part of the InTouch product.)

Windows NT Domain administrators should put procedures in place on all accounts that perform the following:

- Require a minimum number of characters in passwords
- Force the user to change the password after being initially assigned
- Deactivate user accounts after a number of consecutive password failures
- Force the user to change their passwords on a regular basis

The InTouch application will have to be configured to automatically log the user out after a period of inactivity. This is done by using system tags (prefixed by \$) and condition scripts.

Where appropriate, the screen navigation scripts and action scripts should utilize the \$AccessLevel tag to prevent unauthorized entry to specific functionality.

InTouch 7.11 stores the alarm records in the Microsoft SQL™ Server (MS SQL) database, which will need to be configured to maintain an audit trail of all modifications performed to data contained in the database.

Table 2 below describes how the focus application meets the requirements of the regulation. The first column contains the section number of the regulation being reviewed. The second column of the table contains the actual text from the regulation. The third column explains how the focus application will comply with the regulation text.

Table 2

Regulation Section	Regulation Text	How the Regulation Text is Addressed in the Application
B-11.10.a	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	It is the customer's responsibility to ensure each application developed is properly validated.
B-11.10.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.	Historical data and historical alarm records are maintained in a relational database and can be retrieved/printed through a variety of clients (ActiveFactory, Crystal Reports...).
B-11.10.c	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Historical data records are stored by InSQL and cannot be altered. The alarm records are stored by InTouch and held within a relational database, which can be configured for security. Customers are responsible for putting procedures in place to ensure availability.
B-11.10.d	Limiting system access to authorized individuals.	Standard procedures to limit physical access are the responsibility of the customer. InTouch and Windows security are utilized to limit user access to assigned functionality.

Regulation Section	Regulation Text	How the Regulation Text is Addressed in the Application
B-11.10.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.	Historical data records cannot be altered. The alarm records are stored within a relational database, which can be configured to maintain an audit trail detailing the date, time, action taken, and operator, of all data manipulations.
B-11.10.f	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	InTouch supports the ability to enforce interlocks. It is the responsibility of the customer to ensure these system checks are properly implemented.
B-11.10.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.	Both InTouch and Windows security are utilized to limit user access to assigned functionality. InTouch security is utilized to limit user access to screen level functionality while Windows security is utilized to limit operator access to the workstation.
B-11.10.h	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	InTouch security is utilized to limit user access to assigned functionality and InTouch Scripting can be used to limit the scope of a node.
B-11.10.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 responsibility of the customer to ensure that all individuals who develop, maintain or use the systems are properly educated to perform their task.
B-11.10.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 responsibility of the customer to ensure that the policies are in place to hold individuals accountable for actions initiated under their electronic signatures.
B-11.10.k	Use of appropriate controls over systems documentation including:	N/A
	1. Adequate controls over the distribution of, access to and use of documentation for system operation and maintenance.	It is the responsibility of the customer to ensure that the controls are in place to limit 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.	It is the responsibility of the customer to ensure that revision and change control procedures are in place to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

Regulation Section	Regulation Text	How the Regulation Text is Addressed in the Application
B-11.50.a	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:	N/A
	The printed name of the signer	The username of the operator is logged to the database along with all events.
	The date and time when the signature was executed	The date and time is logged to the database along with all events.
	The meaning (such as review, approval, responsibility, or authorship) associated with the signature	The class, type and comment field of the tag to which the event is tied is logged to the database along with all events.
B-11.50.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).	The items identified in paragraphs (a)(1), (a)(2), and (a)(3) are stored in the same databases as mentioned in the above sections and therefore are subject to the same controls as for electronic records.
B-11.70	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.	The event records are maintained in a relational database and utilize an audit trail to prevent falsification. The actual signatures (username and password) are not stored in the database.
C-11.100.a	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	InTouch and Windows security ensure that all username and password combinations are unique.
C-11.100.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 responsibility of the customer to verify the identity of all individuals who will utilize the system.
C-11.100.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.	It is the responsibility of the customer to 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.
C-11.100.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.	It is the responsibility of the customer to 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.	It is the responsibility of the customer to submit the certification to the Office of Regional Operations.
	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 responsibility of the customer to, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

Regulation Section	Regulation Text	How the Regulation Text is Addressed in the Application
C-11.200.a	electronic signatures that are not based upon biometrics shall:	N/A
	1. Employ at least two distinct identification components such as an identification code and password.	Windows security utilizes a username and password.
	1.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.	Windows security requires the user to enter their username and password to gain access to the system. InTouch scripting can be used to require re-authentication of a user's password to complete an action.
	2. Be used only by their genuine owners	It is the responsibility of the customer to put policies and procedures in place that ensure that the electronic signatures are only used by their genuine owners.
	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.	It is the responsibility of the customer to have procedures in place to force users to change their passwords after being initially set by the administrator. This functionality is supported by Windows security.
C-11.200.b	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	This is the responsibility of the customer in the selection of biometrics based mechanism to be used with the system.
C-11.300	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:	N/A
C-11.300.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.	Windows security ensures that all username and password combinations are unique.
C-11.300.b	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Windows security can be configured to enforce password aging.
C-11.300.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 responsibility of the customer to implement 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.

Regulation Section	Regulation Text	How the Regulation Text is Addressed in the Application
C-11.300.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.	Windows security can be configured to disable a users account after consecutive failed logons.
C-11.300.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 responsibility of the customer to perform initial and periodic testing of devices to ensure that they function properly and have not been altered in an unauthorized manner.

Wonderware’s Continuing FDA Development Commitment

Wonderware is committed to a defined product strategy that will lower the cost of development and support for FDA validated applications. This commitment includes the development of 21 CFR Part 11 applications, where the following functions will be addressed:

- Built-in security authentication from a Windows NT Domain, where the configuration is effectively transparent to the user, if he selects to use NT authentication
- The ability to define security models against roles and functions that can be re-used from project to project, thus reducing FDA validation time and maintenance costs
- The ability to report easily on application changes and to do comparisons in order to reduce FDA validation and maintenance costs

These functionalities will be introduced over the next few releases of the InTouch and IndustrialSQL Server products, enabling existing applications to be continued going forward and permitting enhancements to be made to applications with reduced effort for achieving 21 CFR Part 11 compliance.

©2001 Wonderware Corporation. All rights reserved. Wonderware, FactorySuite, InTouch and Avantis are registered trademarks of Wonderware Corporation. ActiveFactory, ArchestrA, FactoryOffice, InTrack, InControl, InBatch, IndustrialSQL Server, MaintenanceSuite, QI Analyst, SCADAAlarm, SuiteVoyager and Web Server are trademarks of Wonderware Corporation. Microsoft and Windows NT are registered trademarks of Microsoft Corporation. All other trademarks are the property of their respective owners.



100 Technology Dr.
Irvine, CA 92618
Tel: (949) 727-3200
Fax: (949) 727-3270
<http://www.wonderware.com>

