Deployment Guide


Authors: Invensys Operations Management and TSD (Total System Design, an Optimization Company)
# Table of Contents by Section

1 Before you Begin
   1.1 About this Guide ................................................................. 3
   1.2 Wonderware References and Documentation ............................... 3
       1.2.1 System Platform 3.1 .................................................. 3
       1.2.2 InTouch 10.1 .......................................................... 4
       1.2.3 Wonderware Historian 9.0 ......................................... 4
       1.2.4 Notes on System Architecture Options ........................... 5
   1.3 Other References & Documentation ....................................... 5
       1.3.1 21 CFR Part 11 ....................................................... 5
       1.3.2 Validation ............................................................ 5
   1.4 Document Conventions ...................................................... 6
   1.5 Glossary .............................................................................. 6

2 The 21 CFR Part 11 Regulation
   2.1 Overview of Part 11 ............................................................ 7
       2.1.1 Subpart B - Electronic Records .................................. 7
           2.1.1.1 Controls for Closed Systems (11.10) ................... 7
           2.1.1.2 Signature Manifestation (11.50) ......................... 8
           2.1.1.3 Signature/Record Linking (11.70) ....................... 8
       2.1.2 Subpart C - Electronic Signatures ................................. 8
           2.1.2.1 General Requirements (11.100) ......................... 8
           2.1.2.2 Electronic Signature Components and Controls (11.200) 9
           2.1.2.3 Controls for Identification Codes/Passwords (11.300) 9
       2.2 Revised Guidance ........................................................... 9
   2.3 Complying with Part 11 ....................................................... 10
   2.4 Compliance Matrix ........................................................... 11

3 Procedural Controls .................................................................. 12
   3.1 Electronic Records - Subpart B .......................................... 12
       3.1.1 Controls for Closed Systems – 11.10 ......................... 12
           3.1.1.1 Validation - 11.10 (a) ..................................... 12
           3.1.1.2 Record Protection - 11.10 (c) ......................... 12
           3.1.1.3 Access Limitations - 11.10 (d) ...................... 13
           3.1.1.4 Audit Trail - 11.10 (e) ................................... 13
           3.1.1.5 Authority Checks - 11.10 (g) ......................... 13
           3.1.1.6 User Qualifications - 11.10 (i) ....................... 13
           3.1.1.7 Accountability - 11.10 (j) .............................. 13
           3.1.1.8 Documentation Control - 11.10 (k) ............... 14
   3.2 Electronic Signatures - Subpart C ...................................... 14
       3.2.1 General Requirements – 11.100 ................................. 14
           3.2.1.1 Signature Uniqueness - 11.100 (a) ................. 14
           3.2.1.2 User Identity - 11.100 (b) ......................... 14
           3.2.1.3 Certification - 11.100 (c) .......................... 14
       3.2.2 Components and Controls – 11.200 ............................. 15
           3.2.2.1 Non-Biometric Signatures - 11.200 (a) ........ 15
       3.2.3 Controls for Identification Codes & Passwords – 11.300 .... 15
           3.2.3.1 ID & Password Uniqueness - 11.300 (a) ....... 15
           3.2.3.2 Password Changes - 11.300 (b) ............... 16
           3.2.3.3 Compromised Devices - 11.300 (c) ............ 16
           3.2.3.4 Transaction Safeguards - 11.300 (d) ......... 16
           3.2.3.5 Device Testing - 11.300 (e) ..................... 16
4 Technological Control

4.1 Electronic Records - Subpart B

4.1.1 Controls for Closed Systems - 11.10

4.1.1.1 Validation - 11.10 (a) ................................................................. 17

4.1.1.1.1 Wonderware Software Verification .............................................. 17

4.1.1.1.2 System Validation ................................................................. 17

4.1.1.2 Record Availability - 11.10 (b) .................................................. 18

4.1.1.2.1 Viewing Recorded Alarms and Events ......................................... 18

4.1.1.2.2 Viewing Recorded Data ......................................................... 18

4.1.1.2.2.1 ActiveFactory Reporting ...................................................... 18

4.1.1.2.2.2 ArchestrA Reporting .......................................................... 18

4.1.1.2.2.3 Wonderware HMI Reports ..................................................... 19

4.1.1.3 Record Protection - 11.10 (c) ...................................................... 19

4.1.1.3.1 InTouch Applications Backup .................................................. 19

4.1.1.3.2 Wonderware Historian Backup ................................................ 20

4.1.1.3.3 Alarm and Event Backup ....................................................... 20

4.1.1.3.4 System Platform Galaxy Backup ............................................. 20

4.1.1.3.5 System Databases Backup .................................................... 20

4.1.1.4 Access Limitations - 11.10 (d) ................................................... 20

4.1.1.4.1 Application Server Security .................................................... 20

4.1.1.4.2 Configuring Secured Write using ArchestrA Security ................. 21

4.1.1.4.3 Configuring Verified Write using ArchestrA Security ............... 22

4.1.1.4.4 InTouch Security ................................................................. 22

4.1.1.4.5 InTouch Secured Write using ArchestrA Based Security ............ 23

4.1.1.4.6 InTouch Verified Write using ArchestrA Based Security .......... 23

4.1.1.4.7 Wonderware Historian Security .............................................. 24

4.1.1.4.8 Alarm and Event Security ..................................................... 25

4.1.1.5 Audit Trail - 11.10 (e) .............................................................. 25

4.1.1.5.1 Capturing System Information and Audit Trails ......................... 25

4.1.1.5.2 Wonderware Historian Modification Tracking ......................... 26, 27

4.1.1.6 Sequencing - 11.10 (f) ........................................................... 28

4.1.1.7 Authority Checks - 11.10 (g) .................................................... 28

4.1.1.8 Device Checks - 11.10 (h) ....................................................... 28

4.1.1.8.1 InTouch Numeric Input Validity Check ...................................... 29

4.1.1.8.2 ArchestrA Numeric Input Validity Check .................................. 29

4.1.1.8.3 Alphanumeric Input Validity Check ......................................... 30

4.1.1.8.4 Data Quality ................................................................. 30

4.1.1.9 Documentation Control - 11.10 (k) .......................................... 31

4.1.2 SIGNATURE MANIFESTATION - 11.50 ....................................... 32

4.1.2.1 Signatures for Alarms and Events ............................................. 32

4.1.2.2 Other Signatures ................................................................. 32

4.1.3 SIGNATURE/RECORD LINKING - 11.70 ..................................... 32

4.1.3.1 Signatures for Alarms and Events ............................................. 32

4.2 Electronic Signatures - Subpart C

4.2.1 General Requirements – 11.100 .................................................. 33

4.2.1.1 Signature Uniqueness - 11.100 (a) ............................................ 33

4.2.2 Components and Controls – 11.200 ............................................. 33

4.2.2.1 Non-Biometric Signatures - 11.200 (a) ...................................... 33

4.2.3 Controls for Identification Codes & Passwords – 11.300 ................. 34

4.2.3.1 ID & Password Uniqueness - 11.300 (a) .................................... 34

4.2.3.2 Password Changes - 11.300 (b) ................................................. 34

4.2.3.3 Transaction Safeguards - 11.300 (d) ........................................... 34

5 Other Technical Products ............................................................... 35, 36

6 About The Co-Author .................................................................... 37

7 References ................................................................................ 37
1. Before You Begin

1.1 About this Guide

Wonderware® prides itself in helping customers reduce the cost and time of application development. In going a step further, Wonderware wants to provide customers from Food and Drug Administration (FDA) audited industries with a set of best practices in regards to the 21 CFR Part 11 requirements.

This 21 CFR Part 11 Deployment Guide for System Platform® 3.1, InTouch® 10.1, and Historian® 9.0 offers information on System Platform, InTouch, and Wonderware Historian features relevant to the 21 CFR Part 11 requirements of the U.S. Food and Drug Administration (FDA). While not directly subject to regulation under 21 CFR Part 11, Wonderware System Platform, InTouch, and Wonderware Historian products incorporate features and functionality designed to facilitate the development of applications for use in FDA regulated industries. Accordingly, Wonderware has developed this document to provide customers with a set of “best practices” in regards to certain Wonderware products and the 21 CFR Part 11 requirements. Best practices suggested in this deployment guide, in conjunction with properly designed and implemented external procedural controls, should reduce cost of development, validation, and re-qualification of applications. However, please note that the methods described in this document represent general guidance and may require adaptation or modification depending on the needs of your specific system implementation. For optimum results, before applying the advice contained in this guide, consult a Wonderware endorsed systems integrator (http://global.wonderware.com/EN/Pages/PartnersSIEndorsedFind.aspx).

Auditing and security functions are tightly integrated with Microsoft® products, and working knowledge of both Microsoft SQL Server® and the Microsoft Windows® operating system is required. It is assumed that you are familiar with administering a Microsoft SQL Server and using the administrative tools provided with the Microsoft Windows Server or Advanced Server® operating system.

For more information on Microsoft SQL Server or the Microsoft Windows operating system, see your Microsoft documentation.

System Platform 3.1, InTouch 10.1 and Historian 9.0 are Wonderware’s products for human-machine interface (HMI) software and a plant historian. They are based on Microsoft Windows and can be used to control and monitor processes in FDA-audited industries. Wonderware Historian is closely linked to Microsoft SQL Server. System Platform, InTouch, Historian, and procedural controls can be used to implement systems that comply with the FDA’s 21 CFR Part 11 regulation.

Readers should note this deployment guide is designed for closed systems. Closed systems are defined as systems where access is controlled by the people responsible for the content of the electronic records. Open systems are not addressed in the scope of this document.

1.2 Wonderware References & Documentation

A PDF file for each of the following guides is typically available on the respective installation CD. You can easily print information from the PDF files. The documentation is also available as online help files through respective application interface or on the Wonderware Developer Network (a valid login is required) https://wdn.wonderware.com/sites/WDN/Pages/Tech_Support/BasicDocumentation.aspx.

1.2.1 System Platform 3.1

The System Platform documentation set includes the following guides:

• System Platform Getting Started Guide.
• Application Server 3.1: Creating and Managing ArchestrA Graphics User’s Guide
• Application Server 3.1: Application Server Scripting Guide
• Application Server 3.1: Platform Manager User’s Guide
  – The Platform Manager User’s Guide provides information on performing runtime administrative tasks and diagnostics on ArchestrA® Application Server platforms and engines.
• Application Server 3.1: Object Viewer User’s Guide
  – This guide describes the user interface and functions of the Object Viewer utility.
• Application Server 3.1: Wonderware Application Server User’s Guide.

- **Application Server 3.1: Galaxy Database Manager User’s Guide**
  - This guide describes the user interface and functions of the Galaxy Database Manager, a part of the ArchestrA System Management Console suite of utilities.

- **Protocol Users Guide**
  - This guide provides background information on the main protocols used between components of Wonderware products.

- **Wonderware FactorySuite A2 Deployment Guide (Updated)**
  - This Wonderware FactorySuite A2 Deployment Guide provides recommendations and ‘best practice’ information so that you can effectively define architectures and design and implement projects in a Wonderware FactorySuite A2 environment.

- **Industrial Application Server Installation Guide - Version 2.0**
  - This document describes how to install one or more components of the Industrial Application Server infrastructure, including the main configuration tool, the Integrated Development Environment (or IDE), and the Galaxy Repository.

### 1.2.2 InTouch 10.1

The InTouch documentation set includes the following guides:

- **Guide to InTouch HMI Documentation**
- **InTouch HMI Concepts and Capabilities Guide**
- **InTouch HMI Application Management and Extension Guide**
- **InTouch HMI Data Management Guide**
- **InTouch HMI Visualization Guide**
- **InTouch HMI SmartSymbols Guide**
- **InTouch HMI and ArchestrA Integration Guide**
- **InTouch HMI Alarms and Events Guide**
- **InTouch HMI Scripting and Logic Guide**
- **InTouch HMI Supplementary Components Guide**
- **InTouch HMI Getting Started Guide**
- **InTouch Protocol Guide**

### 1.2.3 Wonderware Historian 9.0

The Wonderware Historian documentation set includes the following guides:

- **Wonderware Historian 9.0 – Runtime Database Schema**

- **Wonderware Historian 9.0 Administration Guide**
  - This Wonderware Historian Administration Guide provides information on how to administer and maintain an installed Wonderware Historian. This guide describes the tools you will use to administer the Wonderware Historian, as well as how to configure the system to start storing plant data. This guide also describes administration tasks such as changing the default security, configuring system-wide parameters, and monitoring the system.

- **Wonderware Historian 9.0 Concepts Guide**
  - This Wonderware Historian Concepts Guide provides information about the general architecture of the Wonderware Historian system and describes the different subsystems and components that make up the system. This guide can be used as a reference guide for all conceptual information regarding various Wonderware Historian components.

- **Wonderware Historian 9.0 Database Reference.**
  - This Wonderware Historian Database Reference describes the database model of the Wonderware Historian system. Each database entity is described, and the relationships between the entities are defined.

- **Wonderware Historian 9.0 Installation Guide.**
  - This IndustrialSQL™ Server Installation Guide provides information on installing Wonderware Historian, including hardware and software requirements and migration instructions.

- **Wonderware Historian Glossary.**
  - This Wonderware Historian Glossary provides definitions used throughout the Wonderware Historian documentation set.
1.2.4 Notes on System Architecture Options

Wonderware's software components can be used to design industrial IT systems using several architectures, according to the exact requirements of a customer. The choice of architecture can impact the best practices for designing an application to be validated.

The Wonderware System Platform is a suite of products which provides a powerful and common framework for building industrial applications. System Platform integrates security, data quality, communications and alarming within an infrastructure of common services. System Platform also includes Wonderware Historian (formerly known as IndustrialSQL Server) for recording of historical data values, and Wonderware Information Server (formerly SuiteVoyager) as an information portal. InTouch can be used as a visualization client to the System Platform.

InTouch can also be used in a 'stand-alone' mode or as a 'managed application' without System Platform, where the configuration data is stored in a tag database.

Wonderware Historian is a component of System Platform, and can also be used in combination with InTouch tag based applications or in a stand-alone mode, for example when different HMI system(s) are already in place.

Section 4 Technological Control describes Wonderware product features, according to the different architectural options, that support 21 CFR Part 11 compliance.

1.3 Other References & Documentation

1.3.1 21 CFR Part 11

Documentation on 21 CFR Part 11 can be obtained from the following sources:

- Electronic Records; Electronic Signatures Final Rule, 62 Federal Register 13430 (March 20, 1997).
  - This Code of Federal Regulation is the official rule on Electronic Records and Electronic Signatures management for FDA-audited industries.

  - The purpose of this ISPE White Paper is to describe how a risk-based approach to Part 11 could be used to benefit patient health while adversely impacting industry productivity.

  - The purpose of this guidance is to describe the FDA's re-examination of 21 CFR Part 11.

- Complying with 21 CFR Part 11, Electronic Records and Electronic Signatures, Part 2 (September 2001)
  - This document produced by ISPE and PDA was developed to provide a better understanding of 21 CFR Part 11. It aims to provide guidance for the industry on how to comply with the requirements.

  - The purpose of this draft guidance is to describe the FDA's current thinking regarding the time stamp requirements of 21 CFR Part 11.

1.3.2 Validation

- Good Automated Manufacturing Practice (GAMP) 5
  - This document is a guideline, used widely within FDA-regulated industries, for validation of computer systems. ISPE and the GAMP Forum produce the GAMP Guide. (http://www.ispe.org/gamp/)

- General Principles of Software Validation; Final Guidance for Industry and FDA Staff (January 11, 2002).
  - This guidance presents principles of software validation considered to be applicable by the FDA. (http://www.fda.gov/cdrh/comp/guidance/938.html)

- Pharmaceutical cGMPs for the 21st Century: A Risk-Based Approach; A science and risk-based approach to product quality regulation incorporating an integrated quality systems approach (2002).
  - This describes the FDA's review of cGMPs and defines specific immediate, intermediate, and long term steps for the FDA's review. (http://www.fda.gov/oc/guidance/gmp.html)

FDA documents can be downloaded off the FDA's web site at http://www.fda.gov/ and guides developed by ISPE can be bought through ISPE at http://www.ispe.org/.
1.4 Document Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPPERCASE BOLD</td>
<td>Section of the 21 CFR Part 11 requirements</td>
</tr>
<tr>
<td>Bold italics</td>
<td>Text quoted from 21 CFR Part 11</td>
</tr>
<tr>
<td>Initial Capital</td>
<td>Paths and filenames</td>
</tr>
<tr>
<td>Bold</td>
<td>Database names, table names, column names, tag names, command-prompt utilities, menus, commands, dialog box options, programming elements, and text that must be typed exactly as shown.</td>
</tr>
<tr>
<td>Italic</td>
<td>User-supplied variables, relationships, definitions and phrasings.</td>
</tr>
<tr>
<td>Monospace</td>
<td>Code samples, examples, display text and error messages.</td>
</tr>
</tbody>
</table>

1.5 Glossary

This document uses the following terms, abbreviations, and acronyms:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Biometrics</td>
<td>A method of verifying an individual’s physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable</td>
</tr>
<tr>
<td>cGMP</td>
<td>Current Good Manufacturing Practice</td>
</tr>
<tr>
<td>CFR</td>
<td>Code of Federal Regulations</td>
</tr>
<tr>
<td>Closed system</td>
<td>An environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system</td>
</tr>
<tr>
<td>DB</td>
<td>Database</td>
</tr>
<tr>
<td>ER/ES</td>
<td>Electronic Record/Electronic Signature</td>
</tr>
<tr>
<td>FDA</td>
<td>Food and Drug Administration</td>
</tr>
<tr>
<td>GAMP</td>
<td>Good Automated Manufacturing Practice</td>
</tr>
<tr>
<td>Historian</td>
<td>The Wonderware Historian component of the System Platform is a high-performance real-time database for historical information. It combines the power and flexibility of a relational database with the speed and compression of a true process historian, integrating the office with the factory floor or any industrial operation.</td>
</tr>
<tr>
<td>HMI</td>
<td>human-machine interface</td>
</tr>
<tr>
<td>ID</td>
<td>Identification or an item used to verify one’s identity (e.g. user name)</td>
</tr>
<tr>
<td>IDE</td>
<td>Integrated Development Environment</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>InSQL</td>
<td>IndustrialSQL Server</td>
</tr>
<tr>
<td>IndustrialSQL Server</td>
<td>Now called “Wonderware Historian”</td>
</tr>
<tr>
<td>ISPE</td>
<td>International Society for Pharmaceutical Engineering</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>Open system</td>
<td>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</td>
</tr>
<tr>
<td>Part 11</td>
<td>21 CFR Part 11</td>
</tr>
<tr>
<td>SOP</td>
<td>Standard operating procedures</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>System Platform</td>
<td>Wonderware System Platform provides a single platform for all the SCADA, Supervisory HMI, and MES and EMI Software Solutions needs of industrial automation and information personnel.</td>
</tr>
<tr>
<td>UDA</td>
<td>User Defined Attribute</td>
</tr>
<tr>
<td>UTC</td>
<td>Coordinated Universal Time</td>
</tr>
</tbody>
</table>
2. The 21 CFR Part 11 Regulation

Developments in documentation technology, specifically electronic records and electronic signatures, offered companies advantages over paper-based documentation. Companies in regulated industries sought to use these electronic record and electronic signature capabilities to satisfy regulatory requirements.

The United States government responded with guidance in the form of a regulation, 21 CFR Part 11, governing the use of electronic records and electronic signatures needed or used to satisfy FDA requirements.

2.1 Overview of Part 11

The Part 11 regulation contains three major divisions: Subpart A - General Provisions, Subpart B - Electronic Records, and Subpart C - Electronic Signatures. The outline of the regulation is as follows:

- Subpart A - General Provisions
  - 11.1 Scope
  - 11.2 Implementation
  - 11.3 Definition
- Subpart B - Electronic Records
  - 11.10 Controls for closed systems
  - 11.30 Controls for open systems (outside the scope of this guide)
  - 11.50 Signature manifestation
  - 11.70 Signature/record linking
- Subpart C - Electronic Signatures
  - 11.100 General requirements
  - 11.200 Electronic signature components and controls
  - 11.300 Controls for identification codes/passwords

The General Provisions (Subpart A) define what electronic records and electronic signatures must comply with this regulation. The records subject to Part 11 are those in electronic form “created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations.” The regulation also applies to any electronic records submitted to the FDA even if the record is not specifically identified in the FDA regulations. Any signatures applied electronically to such records must also comply with the Part 11 regulations.

The General Provisions also definitively state that electronic records and electronic signatures in compliance with this regulation will be considered the equivalent of paper records and handwritten signatures applied to paper.

2.1.1 Subpart B - Electronic Records

2.1.1.1 Controls for Closed Systems (11.10)

The regulation calls for a series of controls to ensure the authenticity, integrity, and confidentiality (when necessary) of electronic records in closed systems. The scope of this guide is limited, in application, to closed systems. Controls for open systems (21 CFR 11.30) will not be addressed due to this scope focus.
The controls for closed systems are summarized here but addressed in greater detail within sections 3 and 4 of this guide:

- 11.10 (a): Systems must be validated (tested to verify they operate as designed)
- 11.10 (b): Records must be available for inspection in both electronic and human readable form
- 11.10 (c): Records must be protected for retrieval during the required retention period
- 11.10 (d): System access is limited to authorized individuals
- 11.10 (e): Operator entries and actions that create, modify, or delete electronic records must be tracked in a secure, computer-generated audit trail
- 11.10 (f): System checks will enforce sequencing of steps or events
- 11.10 (g): Authority checks will be used to ensure system use or electronic signatures only by authorized individuals
- 11.10 (h): Device checks will determine validity of inputs or operational instructions
- 11.10 (i): System users have the necessary education, training, and experience for their tasks
- 11.10 (j): Written policies that hold individuals accountable for actions initiated by their electronic signatures
- 11.10 (k): Controls over system documentation including access to and changes therein

2.1.1.2 Signature Manifestation (11.50)
Electronic records must include information associated with each electronic signature applied to the record. This information must be controlled to the same degree as the electronic records and all aspects of the signature will be included in the human readable form of the electronic record.

The required signature information includes:
- Printed name of the signer
- Date and time when the signature was applied
- The meaning of the signature (e.g. author, reviewer, approver)

2.1.1.3 Signature/Record Linking (11.70)
Signatures, electronic or handwritten, applied to the electronic records must be linked to the records so they cannot be removed or changed in any way that could be used to falsify records.

Note: This guide does not address the application of handwritten signatures to electronic records.

2.1.2 Subpart C - Electronic Signatures

2.1.2.1 General Requirements (11.100)
There are a number of electronic signature requirements a system must meet to be Part 11 compliant. These requirements are intended to provide evidence and confidence the electronic signatures in the system can be considered the equivalent of handwritten signatures. The general requirements are:

- 11.100 (a): Electronic signatures must be unique to an individual
- 11.100 (b): Organizations must verify an individual’s identity before the individual can use electronic signatures
- 11.100 (c): Persons using electronic signatures must certify to the FDA their electronic signatures are intended to be the legal equivalent of their handwritten signature
2.1.2.2 Electronic Signature Components and Controls (11.200)
The implementation of electronic signatures can be accomplished through biometrics or other means. Specific controls are required on the signature mechanism depending on the method used. Those controls are:

- 11.200 (a): Non-biometric signatures
  - (1): Use at least two different identification components (e.g. user ID and password)
    - (i): Multiple signatures applied by an individual in a continuous session require all electronic signature components for the first signature and only one component for subsequent signatures
    - (ii): Multiple signatures applied by an individual but not in a continuous session require all signature components for each signature
  - (2): Must be used only by their genuine users
  - (3): User administration must be designed to require collaboration of two or more individuals to use another user’s electronic signature

- 11.200 (b): Biometric signatures must be designed so they can only be performed by their genuine owner

2.1.2.3 Controls for Identification Codes/Passwords (11.300)
Systems using a combination of identification code (e.g. user ID) and password as the electronic signature components must ensure the integrity of these signatures through a series of controls.

- 11.300 (a): Maintain user ID and password combinations so no two individuals can have the same combination
- 11.300 (b): Codes and passwords are periodically checked or revised
- 11.300 (c): Lost or potentially compromised identification devices (e.g. tokens, cards) or passwords are voided and replaced with a new equivalent
- 11.300 (d): Transaction safeguards are used to prevent unauthorized use of IDs or passwords
- 11.300 (e): ID or password generating devices (e.g. tokens) must be tested initially and periodically to ensure they are unaltered and function properly

2.2 Revised Guidance
The release of Part 11 by the FDA was intended to permit the extensive use of electronic technology in a manner consistent with the FDA’s need to protect public health. The result was a significant amount of discussion within the industry requiring the subsequent release of a compliance policy guide and draft guidance for the following: validation, glossary of terms, time stamps, maintenance of electronic records, and electronic copies of electronic records.

While the intent was to produce a wide use of technology, concerns about Part 11 developed within the industry to the point where the regulation was perceived as having the opposite effect (see ISPE White Paper for examples).

In February of 2003 the FDA issued draft Part 11 guidance with a final guidance following in August 2003. In this final guidance, the FDA presented the group’s intention to limit the scope and application of Part 11. Specific industry concerns about Part 11 were noted in this final guidance:

- Unnecessarily restricts the use of electronic technology inconsistent with the regulations intent
- Can significantly increase the costs of compliance due to the Part 11 requirements
- Discourages innovation and technological advances without providing significant public health benefit
The revised guidance is intended by the FDA to address these industry concerns as the result of the original Part 11 regulation was the opposite of the intent. The emphasis within this revised guidance is clear:

- FDA is re-evaluating Part 11 as it applies to FDA regulated products
- Part 11 remains in effect
- The FDA will narrowly interpret the scope of Part 11
  - Fewer records will be subject to Part 11
  - Part 11 will apply to:
    - Records required to be maintained by predicate rule(s) that are in electronic format in place of paper
    - Records required to be maintained by predicate rule(s) that are in electronic format in addition to paper format and are relied upon to perform regulated activities
    - Records submitted to FDA under predicate rules
    - Electronic signatures that are the equivalent to handwritten signatures required by predicate rule (e.g. reviewed, approved, verified)
- Enforcement discretion will be used during the period of re-examination
  - FDA does not intend to take enforcement action to enforce compliance with the validation, audit trail, record retention, and record copying requirements of Part 11 as explained in the final guidance
  - Records must still be maintained or submitted consistent with the applicable predicate rules
- No requirements will be enforced for systems that were operational before August 20, 1997, the effective date of Part 11

The enforcement discretion is strictly limited to the Part 11 requirements but some of these aspects of a system may still apply to satisfy the predicate rules. Regarding the areas identified for enforcement discretion, Part 11 should be viewed as not adding to or increasing the regulatory requirements defined in other regulations. Part 11 does not remove or invalidate existing requirements defined in other regulations. For example, system validation is still required for some systems by 21 CFR 820.70(i).

2.3 Complying with Part 11

The first step to compliance with Part 11 is to determine if Part 11 applies to the system in question and if it does, which parts of Part 11 apply. For example, an electronic records system that does not include electronic signatures does not need to comply with Subpart C. Each company needs to make a determination for each new system based on their understanding and application of Part 11. The ISPE and PDA guide also provides guidance for understanding and complying with Part 11. Whatever decision is made, this determination should be clearly documented and consistent with a company's SOPs related to regulatory requirements.

Once a system is found to require Part 11 compliance, the company needs to determine how to comply with the applicable requirements. This requires a mixed solution of two types of controls: technological and procedural. Some specific requirements may even be addressed by both types of controls.

The presence of procedural requirements means that no technological solution, software, etc. can be compliant with the Part 11 regulation as it exists on its own. This guide will focus on the application of technological controls, but will also identify where procedural controls are required.
## 21 CFR 11 Requirement Matrix

<table>
<thead>
<tr>
<th>21 CFR 11 Requirement</th>
<th>Procedural</th>
<th>Technological</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subpart B 11.10</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Subpart B 11.10 (a)*</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Subpart B 11.10 (b)*</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Subpart B 11.10 (c)*</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Subpart B 11.10 (d)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Subpart B 11.10 (e)*</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Subpart B 11.10 (f)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Subpart B 11.10 (g)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Subpart B 11.10 (h)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Subpart B 11.10 (i)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Subpart B 11.10 (j)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Subpart B 11.10 (k)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Subpart B 11.10 (k) 1</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Subpart B 11.10 (k) 2*</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Subpart B 11.30*</td>
<td>N/A**</td>
<td>N/A**</td>
</tr>
<tr>
<td>Subpart B 11.50 (a)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Subpart B 11.50 (a) 1</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Subpart B 11.50 (a) 2</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Subpart B 11.50 (a) 3</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Subpart B 11.50 (b)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Subpart B 11.70</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Subpart C 11.100 (a)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Subpart C 11.100 (b)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Subpart C 11.100 (c)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Subpart C 11.100 (c) 1</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Subpart C 11.100 (c) 2</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Subpart C 11.200 (a)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Subpart C 11.200 (a) 1</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Subpart C 11.200 (a) 1.i</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Subpart C 11.200 (a) 1.ii</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Subpart C 11.200 (a) 2</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Subpart C 11.200 (a) 3</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Subpart C 11.200 (b)</td>
<td>N/A***</td>
<td>N/A***</td>
</tr>
<tr>
<td>Subpart C 11.300</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Subpart C 11.300 (a)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Subpart C 11.300 (b)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Subpart C 11.300 (c)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Subpart C 11.300 (d)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Subpart C 11.300 (e)</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

* These sections are part of the enforcement discretion defined in the Part 11 Guidance for Industry
** Open systems are outside the scope of this guide
*** Biometric signatures are outside the scope of this guide

### 2.4 Compliance Matrix

This table identifies which type of control is needed to comply with specific requirements defined in the Part 11 regulation. An ‘X’ in the Procedural or Technological column indicates the control applies for the requirement listed in that row. Sections 3 and 4 of this guide are structured to mirror the regulation and present the reader with information and specific technical methods or options available to support Part 11 compliance. In each subsection within Sections 3 and 4, the specific regulation text being addressed is presented to aid in the interpretation and application of this guide (shown in **bold italics**).
3. Procedural Controls

Procedural controls must be applied as part of any Part 11 solution. These procedural controls are outside the scope of Wonderware's products and offerings to the industry but this guide addresses the procedural controls and provides some content to aid a company's efforts to understand and apply the necessary procedural controls.

3.1 Electronic Records - Subpart B

3.1.1 Controls for Closed Systems - 11.10

21 CFR Part 11:
“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:”

Companies need to define and execute a system with components (e.g. SOPs, processes, tools) that will ensure the closed system controls are properly established and maintained. Periodic verification, or auditing, of the controls should be performed to maintain the integrity of the controls, once established.

3.1.1.1 Validation - 11.10 (a)

21 CFR Part 11:
“(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.”

Validation is one of the requirements where enforcement discretion will be applied. In this area, that means validation of electronic record/electronic signature (ER/ES) systems will not face any new requirements due to the Part 11 record. System validation must still be performed in compliance with the predicate rule (21 CFR 820.70(i)).

This validation should follow a defined methodology. The GAMP5 guide recommends important validation principles for companies to consider using. Significant procedural activities to perform include defining requirements, documenting system design, and testing that the system performs as defined by the design – including documenting this testing or verification.

3.1.1.2 Record Protection - 11.10 (c)

21 CFR Part 11:
“(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.”

The following procedural actions should be performed to protect and enable record retrieval:

- Define procedures for providing records to internal and external parties
- Specify retention requirements – specifically the retention period
- Define backup, recovery, archival, and retrieval processes for electronic records

This is another area where enforcement discretion will be applied but this discretion is specifically limited to generating copies of records. Electronic records should be available at a company's facility using that company's defined tools and methods or the records should be made available as copies in some common format (e.g. PDF, XML).
3.1.1.3 Access Limitations - 11.10 (d)

21 CFR Part 11:
“(d) Limiting system access to authorized individuals.”

Procedures need to be defined that address system user administration, including who should be granted access and how that access is granted. Often systems require administrator level or otherwise high level users with great latitude in the actions they can perform within the system. These high level users should get special attention when considering rules, limitations, and other procedural safeguards that can be applied.

Some customers may interpret the Part 11 guidelines to require a record of changes to user access profiles. Wonderware software does not record these changes so, if required, a manual procedure should be established to create and maintain these records.

3.1.1.4 Audit Trail - 11.10 (e)

21 CFR Part 11:
“(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.”

Reliability of records must still be maintained even though an audit trail may not be specifically required due to the FDA’s enforcement discretion defined in the revised guidance. Procedures should be established that require documentation of the methods for ensuring reliable records, whether this includes an audit trail or not.

3.1.1.5 Authority Checks - 11.10 (g)

21 CFR Part 11:
“(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.”

Procedures need to define how systems should perform authority checks. If any variation in authorization method is allowed, the specific scenarios and authorization methods for each must be specifically defined.

This requirement is related to the access limitation requirement (section 3.1.1.3). However, this requirement addresses allowing specific actions within the system whereas the access limitation requirement relates to general access to the system.

3.1.1.6 User Qualifications - 11.10 (i)

21 CFR Part 11:
“(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.”

The method or methods used to determine persons who are qualified to interact with ER/ES systems must be defined.

3.1.1.7 Accountability - 11.10 (j)

21 CFR Part 11:
“(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.”

Policies need to define the responsibilities of those users with electronic signature capabilities. This should include any consequences or other deterrents for misuse of the electronic signature function by those users. This requirement is intended to ensure electronic records can be trusted as signed.
3.1.1.8 Documentation Control - 11.10 (k)

21 CFR Part 11:
“(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.”

The controls placed on system documentation must be defined by procedures. Requirements for recording and tracking system documentation changes must also be defined.

3.2 Electronic Signatures - Subpart C

3.2.1 General Requirements - 11.100

3.2.1.1 Signature Uniqueness - 11.100 (a)

21 CFR Part 11:
“(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.”

Procedures should be established to ensure an electronic signature is unique and can only be used by one individual. Companies should also be prepared, with defined procedures, to handle situations where signature authorities are not available because no others can execute a signature on their behalf. A valid remedy is to establish rules for delegation of signature responsibility so work flow can progress even if primary signature authorities are not available to execute an electronic signature.

3.2.1.2 User Identity - 11.100 (b)

21 CFR Part 11:
“(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.”

Verification of an individual’s identity is a procedural activity. The process or methods of verification should be documented.

3.2.1.3 Certification - 11.100 (c)

21 CFR Part 11:
“(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.”

Certifying the persons using electronic signatures are intending to apply the legal equivalent of a handwritten signature is also only a procedural activity. This certification is applicable to all systems where a certified person is able to apply electronic signatures. Certifications are required for each person and not each system.
3.2.2 Components and Controls - 11.200

3.2.2.1 Non-Biometric Signatures - 11.200 (a)

21 CFR Part 11:

“(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.

(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.”

Procedures should be established to define what distinct identification components are considered valid for use in an electronic signature. These procedures should also define what is considered a continuous period of controlled access for the purpose of identifying when only one electronic signature component is required for subsequent signings.

These procedures also need to ensure persons only use or apply their own electronic signature and they do not share or distribute any components of their electronic signature such that others cannot falsely sign electronic records for them.

Finally, the procedures need to define and manage signature components such that a single person cannot attempt to use another’s signature. For example, if the system administrator, who knows the user identification codes assigned, can also reset a person’s password to a known value then that individual could falsify signatures for others without requiring any assistance from others.

3.2.3 Controls for Identification Codes & Passwords - 11.300

21 CFR Part 11:

“**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:**”

ID and passwords are given specific mention in the regulation as they are by far the most commonly used electronic signature components.

3.2.3.1 ID & Password Uniqueness - 11.300 (a)

21 CFR Part 11:

“(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.**”

This requirement is most likely addressed by the procedures required for electronic signature uniqueness in 21 CFR 11.100(a).

One possible additional consideration is that rules for password components can be used to make passwords more difficult to guess. For example, password length of 6 or more characters, at least one capital letter, at least one letter and one number, would all contribute to making it more difficult to guess another’s password.
3.2.3.2 Password Changes - 11.300 (b)

21 CFR Part 11:

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

Identification codes should be disabled for users that are no longer allowed access to a system. Users should be periodically reviewed to ensure they are currently assigned to the correct user groups as many systems grant access or permissions based on membership in defined user groups. These types of changes are often due to change in roles or separation from the company. Whatever method is applied, the procedures should not jeopardize the integrity of signatures already executed which means it may not be possible to completely remove a user from the system.

Passwords are commonly required to be periodically changed in an effort to minimize the likelihood an ID-password combination can be compromised. This generally accepted practice is especially important in ER/ES systems. Additional rules, such as password cannot be changed to be the same as the user ID, passwords cannot be reused or reused within a specific time period, and others should also be considered to protect the integrity of passwords.

3.2.3.3 Compromised Devices - 11.300 (c)

21 CFR Part 11:

“(c) Following loss management procedures to electronically deauthorize 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.”

Loss management procedures must be clearly defined and consistently applied to protect the integrity of electronic signatures when passwords or any other signature component or component generating device is lost or compromised.

3.2.3.4 Transaction Safeguards - 11.300 (d)

21 CFR Part 11:

“(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.”

Procedures should define how to handle any unauthorized attempts to use a person's ID and/or password. This will depend on the technological controls to identify the unauthorized attempted use.

3.2.3.5 Device Testing - 11.300 (e)

21 CFR Part 11:

“(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.”

Procedures need to define the testing to perform and when it should be performed, including the frequency of the periodic tests.
4 Technological Control

4.1 Electronic Records – Subpart B

4.1.1 Controls for Closed Systems – 11.10

21 CFR Part 11:

“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:”

4.1.1.1 Validation - 11.10 (a)

21 CFR Part 11:

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

4.1.1.1.1 Wonderware Software Verification

FDA-audited industries are required to properly validate their applications. The software world uses the term validation and verification interchangeably. However, according to the document General Principals of Software Validation; Final Guidance for Industry and FDA Staff, Wonderware provides software that is verified. The partial definition of software verification in the FDA document is:

Software verification provides objective evidence that the design outputs of a particular phase of the software development life cycle meet all of the specified requirements for that phase. Software verification looks for consistency, completeness, and correctness of the software and its supporting documentation, as it is being developed.[…]

All Wonderware products are verified and tested extensively prior to release. Furthermore, Wonderware’s commitment to quality ensures performance reliability.

Software validation is for a finished device or system hence it does not apply to Off-the-Shelf configurable software like Wonderware products. Validation applies to systems created using the configurable Wonderware products.

4.1.1.1.2 System Validation

Validation of the applications created using the Wonderware products is entirely the responsibility of the FDA-audited industry. Creating and maintaining a validated state is simplified by features and capabilities within the Wonderware products.

For example, InTouch includes standard user entry windows for both alphanumeric and numeric entries. These standard windows provide entry capabilities as part of the off-the-shelf products so the features do not need validation. It is only necessary to consider validating the connections to these windows to prove entered values end up in the right place within the system.

Another example, graphic object templates can be used to create templates for user interface objects like control valves or process variable displays. The features of each template are defined once and then the template can be reused each time an object with the defined features is needed. Use of the template simplifies validation by reducing the scope of testing for this custom-configured item. All features of the object template should be tested fully once but each instance of the template does not require full testing of all the template features because each individual instance shares the features of the template. Validation of each instance of a template can focus on the custom configuration of the specific instance – e.g. linking of the object to a specific system input or output.

Decisions to reduce testing scope are completely within the boundaries of currently accepted industry methodology. GAMP 5 specifically promotes the use of a risk-based approach to validation, including testing. Capabilities within the Wonderware products like those mentioned above provide a strong case of reduced testing when properly employed within a custom-configured system.
4.1.1.2 Record Availability - 11.10 (b)

21 CFR Part 11:
“(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.”

4.1.1.2.1 Viewing Recorded Alarms and Events

Wonderware provides the Alarm DB View ActiveX control and the Alarm View ArchestrA Symbol to visualize data from the alarm database in an InTouch application. This control is used to show all alarm and event information generated from an InTouch application or from an ArchestrA Galaxy during run time.

For information on configuring the Alarm DB View ActiveX control, see “Viewing Recorded Alarms” in Chapter 10 of the InTouch HMI Alarms and Events Guide.

4.1.1.2.2 Viewing Recorded Data

Wonderware offers products that can be linked to various report generators. Report generators get data through queries to databases. All Wonderware software is tested to ensure data stored in the databases are accurate and complete.

Provided the chosen report generator is properly configured, the reports generated should contain an accurate and complete set of data.

4.1.1.2.2.1 ActiveFactory Reporting

The ActiveFactory Reporting Website is a preconfigured Wonderware Information Server component that allows web users to:
• Generate reports using data from Wonderware Historian databases.
• Trend history data from Wonderware Historian databases.
• Build and execute SQL queries against data from Wonderware Historian and other databases.

The ActiveFactory Reporting Website can be accessed either directly or through Wonderware Information Server. When accessing the site directly, a custom starting page appears from which users can access the various Reporting Website features. When accessing through Wonderware Information Server, the reporting Website features appear under the ActiveFactory node in the Launch Pad. Although not required, you may want to change some of the settings related to report publishing. This can be accomplished by editing a set of .xml files.

For information on using ActiveFactory Reporting, see “ActiveFactory Reporting” in Chapter 18 of the Wonderware Information Server Administration Guide.

4.1.1.2.2.2 ArchestrA Reporting

ArchestrA Reporting is a set of features that publish reports using Wonderware Information Server, Wonderware Historian, and other system data. ArchestrA Reporting integrates Microsoft SQL Server Reporting Services with Industrial Application Server. You can use ArchestrA Reporting features to provide reports on data stored by a variety of Wonderware products and to view these reports from a web browser.

For information on using ArchestrA Reporting, see “Using ArchestrA Reporting” in Chapter 19 of the Wonderware Information Server Administration Guide. For general information on using SQL Server Reporting Services, see the Microsoft documentation.
4.1.1.2.2.3 Wonderware HMI Reports

Wonderware HMI Reports is a product that allows creation and delivery of reports from an InTouch application, a Wonderware Historian database or third party data sources.

You can use Wonderware HMI Reports features to provide reports on data stored by a variety of Wonderware products and to view these reports in Adobe Acrobat reader, Microsoft Excel or from a web browser.

For information on using Wonderware HMI Reports, see the product documentation.

4.1.1.3 Record Protection - 11.10 (c)

21 CFR Part 11:
“(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.”

Protection of records includes performing scheduled backups of data. Typically backups should made and maintained for InTouch applications, System Platform Galaxy, Wonderware Historian history blocks and SQL Server tables, WWALMDB alarm and event database and any other system databases.

4.1.1.3.1 InTouch Applications Backup

In architectures where InTouch applications are based on tags defined in the tag-database (as opposed to using a plant model in System Platform), Wonderware InTouch applications can be either Stand-Alone or Managed. Backups for Stand-Alone InTouch applications must be made and maintained manually by selecting and copying the application directory.

Managed InTouch applications are maintained using the ArchestrA Integrated Development Environment (IDE) if it is installed on the same computer as the InTouch HMI. Unlike stand-alone InTouch applications that are managed entirely by InTouch Application Manager, managed applications are more integrated into the ArchestrA environment. Managed InTouch applications appear in the InTouch Application Manager as “Managed” and can be edited only by starting WindowMaker from within the IDE. Backups for managed InTouch applications are maintained in the System Platform Galaxy and are backed up with all of the other ArchestrA objects.

Managed InTouch applications are preferred where they will be deployed into regulated environments. A Managed InTouch application uses the IntouchViewApp object to manage the synchronization and delivery of files required by the associated InTouch application. The advantages of this managed application choice are all changes are recorded and comments are allowed when changes are made. For more information, see Chapter 1, About InTouch and ArchestrA Integration, in the InTouch HMI and ArchestrA Integration Guide.

Wonderware InTouch includes an application version feature - a system tag that increments each time something is changed in the InTouch application configuration. This tag is called $ApplicationVersion. $ApplicationVersion can be a valuable asset in the validation process because it can be recorded in the validation protocols to ensure validated application has not been changed or altered.

Figure 1:
Selecting the InTouch $ApplicationVersion Tag
4.1.1.3.2 Wonderware Historian Backup

Wonderware Historian is constituted of two entities requiring backup: the SQL Server runtime database, and history blocks. Each of these entities has a separate backup procedure. For runtime database and history block backups see, “Managing the Wonderware Historian Runtime Database” and “Managing Wonderware Historian History Blocks” in Chapter 5, “Managing Data Storage” in the Wonderware Historian Administration Guide.

4.1.1.3.3 Alarm and Event Backup

Management of the alarm database is performed using two InTouch utilities. The Alarm DB Purge-Archive utility is used to remove records from the database permanently or archive them to files. If the database becomes corrupt, use the Alarm DB Restore utility to restore archived records. For instructions on using these utilities see, “Maintaining the Alarm Database” in Chapter 12 of the InTouch HMI Alarms and Events Guide.

4.1.1.3.4 System Platform Galaxy Backup

The configuration model of a System Platform application is stored in the Galaxy Repository, which is an MS SQL Server database. The backup function of the Galaxy Database Manager archives all files and configuration data required to recreate the selected Galaxy in an empty Galaxy Repository. For procedures on backing up a Galaxy see, “Backing Up a Galaxy” in Chapter 2, “Using the Galaxy Database Manager,” in the Galaxy Database Manager User’s Guide.

4.1.1.3.5 System Databases Backup

For backup of data stored in other system databases, in your case Microsoft SQL Server, see your Microsoft Documentation.

4.1.1.4 Access Limitations - 11.10 (d)

21 CFR Part 11:
“(d) Limiting system access to authorized individuals.”

4.1.1.4.1 Application Server Security

The ArchestrA security system is a global function that applies to every object in the Galaxy database. It is a relationship-based security system between users and the objects and functions of the Galaxy.

ArchestrA security is designed to allow system administrators to easily define users and assign the operations they are allowed to perform. The security permissions are defined in terms of the operations the users can perform using automation objects.

FDA-audited industries should use the OS User Based or OS Group Based Security model for best results. Both OS Security models use Windows operating system authentication. This permits user name and password management, outside InTouch, directly in the Windows operating system environment. By using OS Security you benefit from the standard Windows functions for password aging, logon maximum trial, user name uniqueness and more.

If using OS Group Based Security Authentication Mode, make sure there is an understanding of the Windows operating system, particularly its user permissions, groups and security features. ArchestrA OS Group-based security uses these Windows features. For more help, see the Microsoft online help or a 3rd-party book about Windows security.
When using local OS Groups as Roles, each node within a Galaxy must have the same OS Users, Groups, and user-group mappings to get the same level of access to the user at each node. In order to avoid this in regulated environments the use of a Windows Domain controller and Windows Active Directory is recommended in multiple node installations.


ArchestrA-based security includes advanced security mechanisms that also affect InTouch.

4.1.1.4.2 Configuring Secured Write using ArchestrA Security

Attributes in an ArchestrA Galaxy can be configured to have an access control as Secured Write. Secured Write attributes require users to re-enter their passwords to complete the write back.

Figure 3: Configuring Secured Write using ArchestrA Security
4.1.1.4.3 Configuring Verified Write using ArchestrA Security

Attributes in an ArchestrA Galaxy can be configured to have an access control as Verified Write. Verified Write attributes require users to re-enter their passwords and also authorization of a second operator to complete the write back.

Figure 4: Configuring Verified Write using ArchestrA Security

4.1.1.4.4 InTouch Security

When using InTouch in architectures based on tag databases, InTouch offers multiple security configurations. FDA-audited industries should use the OS Security model for best results. OS Security model uses Windows operating system authentication. This permits user and password combination management, outside InTouch, directly in the Windows operating system. By using OS Security, you benefit from existing functions for password aging, logon maximum trial, user name uniqueness and more.


InTouch also offers an option for ArchestrA based security. When an InTouch node is configured to use ArchestrA security, the InTouch HMI uses methods and dialog boxes from Application Sever for logon and logoff operations. Users are configured in the Application Server IDE. An InTouch application configured to use ArchestrA security provides the additional functions which are useful in a regulated environment.
4.1.1.4.5 InTouch Secured Write using ArchestrA Based Security

Writing to an ArchestrA attribute that is configured for Secured write in InTouch requires users a user to re-enter their passwords to complete the write back. The InTouch popup that is displayed when modifying a Secured Write attribute is shown below.

![InTouch Secured Write using ArchestrA Security](image)

4.1.1.4.6 InTouch Verified Write using ArchestrA Based Security

Writing to an ArchestrA attribute that is configured for Verified write, in InTouch requires users a user to re-enter their passwords and also authorization of a second operator to complete the write back. The InTouch popup that is displayed when modifying a Verified Write attribute is shown below.

![InTouch Verified Write using ArchestrA Security](image)
4.1.1.4.7 Wonderware Historian Security

Wonderware Historian uses two security mechanisms:

- Windows operating system security
- Microsoft SQL Server security

Wonderware Historian uses Microsoft SQL Server security configured in SQL Server Authentication mode or Mixed mode. Mixed mode allows users to connect to an instance of SQL Server using either Windows authentication or SQL Server Authentication.

The security choice from either SQL Server Enterprise Manager or Wonderware Historian Console is offered when registering a server. FDA-audited industries should use Mixed mode and Windows Authentication. Windows Authentication offers consistency with the Wonderware OS Security models. SQL Server allows you to define Windows user groups as SQL Server users thus ensuring centralization of all user related information and facilitating management of all parameters.

When the Wonderware Historian is installed, default SQL Server logins are created that can be used for logging on to the historian from client applications. These default logins provide “out of the box” functionality so that logins do not have to be created to start using the system. The following table describes the preconfigured logins:

<table>
<thead>
<tr>
<th>Login Name</th>
<th>Password</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaAdmin</td>
<td>pwAdmin</td>
<td>A user who can access and modify all data and create objects. Cannot drop the database or truncate tables.</td>
</tr>
<tr>
<td>aaPower</td>
<td>pwPower</td>
<td>A user with full read access and the ability to create objects and modify the contents of the non-core tables</td>
</tr>
<tr>
<td>aaUser</td>
<td>pwUser</td>
<td>A read-only user who can access all data, but cannot modify data or consume database resources</td>
</tr>
<tr>
<td>aadbo</td>
<td>pwddbo</td>
<td>Database owner. Full permissions</td>
</tr>
</tbody>
</table>

Applications that are deployed in FDA regulated industries should always change the default passwords for the Wonderware generated SQL Server logins.


For more information on server registration, see “Registering Wonderware Historian” in Chapter 1, “Getting Started with Administrative Tools,” in the Wonderware Historian Administration Guide.

For a more secure installation, check the “Always prompt for login” information check box in the Registered Wonderware Historian Properties window.

For information on SQL Server security and registration, see your Microsoft SQL Server documentation.
4.1.1.4.8 Alarm and Event Security

The Wonderware InTouch Distributed Alarm system includes the Alarm DB Logger utility that logs alarms and events to an alarm database. The Wonderware Alarm DB Logger Manager uses fixed accounts in the Microsoft SQL Server database to access the data. The DB Logger needs to have a write-access account which is specified using the Alarm DB Logger manager utility.

The fixed user accounts (names and passwords) present a possible compliance risk. Companies should consider the potential for un-audited changes to the alarm database and determine if any procedural controls should be employed to address the potential risks. These procedural controls could include limiting access to the database by isolating the system network and databases from the corporate network and/or physical limitations to HMI s that can access the alarm database.

4.1.1.5 Audit Trail - 11.10 (e)

21 CFR Part 11:
"(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.”

4.1.1.5.1 Capturing System Information and Audit Trails

All InTouch and ArchestrA tags defined as alarms are logged in the wwalmdb database. When an InTouch alarm provider (e.g. InTouch or ArchestrA) is configured to use either operating system or ArchestrA authentication and an alarm occurs, the alarm record contains the full name of the operator, assuming the operator is logged on, along with the time and date and alarm details. If the alarm is subsequently acknowledged, and the node performing the acknowledgement is set to use operating system or ArchestrA security, the alarm record contains the full name of the acknowledgement operator. Otherwise, the alarm record contains a computer name concatenated with whatever is in the $Operator tag.

All tags that are configured as events have a record logged in the wwalmdb database each time an action happens with it or its value is changed. All event records, in the wwalmdb database, are logged with the full name of the logged on user and a time stamp in UTC. Logging the operator with an event can be forced by using ArchestrA secured and verified write attributes as described in section 4.1.1.4.1.

A comment field can also be configured in InTouch or ArchestrA and logged along with the alarm or event.

This logging of alarms and events that occurs while running a system can be used to create a report of system operation. In a production environment this information could be used to generate a batch report, which could be an electronic record, that showed alarms and events (e.g. setpoint changes, user logon/off) during a batch or production run.

This information logged into the database could be part of an electronic record about system operation. While this is helpful information related to system operation, it does not constitute an audit trail.

An audit trail would be a record of any changes (additions, deletions, or modifications) to this data once it has been logged. For example, if another system operator changed an alarm limit value (a logged event) while someone else was logged in then the event recording that value change could be changed in the electronic record to indicate the actual operator making the change. That change to the electronic record would be subject to tracking in an audit trail.

SQL Server can be configured, by using triggers, to track and log changes made to any data, see the Microsoft SQL Server documentation.
4.1.1.5.2 Wonderware Historian Modification Tracking

The Wonderware Historian supports tracking of modifications (inserts and updates) to columns in the Runtime database. Modification tracking can be used to track changes to configuration data and changes to actual historian data. The Wonderware Historian uses the same security defined for SQL Server for inserting and updating data. However, data values cannot be deleted from storage.

Modification tracking is system-wide; it is controlled via the use of the ModLogTrackingStatus system parameter. Modification tracking stores a record of modification events that include the old data, the new data and the user name of the user registered with Windows Authentication in the Wonderware Historian Console. Information in the modification tracking tables is stored in the data files of the Microsoft SQL Server database.
There are two types of modifications that can be tracked:

- Changes to configuration data. For example, additions or changes to tag, I/O Server, and storage location definitions. For more information, see “Modification Tracking for Configuration Changes” in the *Wonderware Historian Concepts Guide*.

- Changes to history data. For example, data inserts and updates via Transact-SQL statements or CSV imports. For more information, see “Modification Tracking for Historical Data Changes” in the *Wonderware Historian Concepts Guide*.

---

**Figure 9:** Modification Tracker Example
4.1.1.6 Sequencing - 11.10 (f)  
21 CFR Part 11:  
“(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.”

Wonderware products can be configured to perform and enforce operational checks and sequencing of steps and events with the use of scripting and ArchestrA objects. Wonderware provides a Sequencer ArchestrA object that can be used to facilitate the configuration and verification of operational checks and sequencing of steps and events.

The compliance of these operations is up to the developer and should be verified during the testing and qualification phases of a project.

4.1.1.7 Authority Checks - 11.10 (g)  
21 CFR Part 11:  
“(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.”

The Wonderware features relevant to authority checks are the same as those discussed previously in 4.1.1.4 Access Limitations - 11.10 (d).

4.1.1.8 Device Checks - 11.10 (h)  
21 CFR Part 11:  
“(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.”
4.1.1.8.1 InTouch Numeric Input Validity Check

Wonderware InTouch can be used to validate source data. The Analog User Input Touch Link can be used to verify that user input is within an allowable range. The figure below shows the Touch Link animation properties window. By entering a Min Value and Max Value user entries of analog data can be forced within a certain range.

![Figure 11: InTouch Analog User Input Touch Link](image1)

4.1.1.8.2 ArchestrA Numeric Input Validity Check

ArchestrA symbols can also be used to validate source data. The User Input Animation can be used to verify that user input is within an allowable range. The figure below shows the User Input Link animation properties window. By checking the Restrict Values check box and entering Minimum and Maximum values user entries of analog data can be forced within a certain range.

![Figure 12: ArchestrA User Input Animation](image2)
4.1.1.8.3 Alphanumeric Input Validity Check

The examples above illustrate the validation of user entered data that is analog. String data can be checked and validated using scripting functions in both InTouch and ArchestrA. Below is an example script that can be executed as an action animation, data change script or any other method. This example checks a user string entry for length and any illegal special characters. It can easily be modified to perform other validation actions.

```
Error = 0;
ASCIICode = 0;

IF TestString01 <> "" THEN
   FOR Index = 1 TO StringLen(TestString01)
      ASCIICode = StringASCII(StringMid(TestString01,Index,1));
      IF (ASCIICode >= 48 AND ASCIICode <= 57) OR (ASCIICode >= 65 AND ASCIICode <= 90) OR (ASCIICode >= 97 AND ASCIICode <= 122) THEN
         Error = 0;
      ELSE
         MessageBox("Entry contained illegal characters. Only alpha-numerics, underscores and dashes are allowed!","Illegal Characters Found",10);
         Error = ASCIICode;
         EXIT FOR;
      ENDIF;
   NEXT;
ELSE
   Error = 9999;
   MessageBox("Entry cannot be null!","Invalid Entry",10);
ENDIF;
TestString01 = "";

4.1.1.8.4 Data Quality

Wonderware System Platform maintains a data quality attribute for all tags. Data quality is the degree of validity for a data value. Data quality can range from good, in which case the value is exactly what was originally acquired from the plant floor, to invalid, in which the value is either wrong or cannot be verified. As a data value is acquired, stored, retrieved, and then shown, its quality can degrade along the way, as external variables and events impact the system.

Wonderware InTouch and ArchestrA can make use of the IsGood() and IsBad() functions to test the quality of data and make decisions based on the results. See InTouch HMI Data Management Guide and the Creating and Managing ArchestrA Graphics User’s Guide for more information on using the data quality attribute.

Wonderware Historian can use the data quality attribute in its data logging operations. This allows systems to identify any invalid data that has been logged or captured as part of an electronic record. See the Wonderware Historian Concepts Guide for more information on how the Wonderware Historian utilizes data quality information.
4.1.1.9 Documentation Control - 11.10 (k)

21 CFR Part 11:
“(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.”

Wonderware System Platform is configured with the ArchestrA IDE. This application provides a secure environment for developing and maintaining a system configuration. Galaxies deployed in regulated environments should employ OS User based or OS Group based security. All aspects of application development will then be controlled by a combination of Microsoft Windows and Galaxy security. See the Wonderware Historian Concepts Guide for more information on how the Wonderware Historian utilizes data quality information.

For more information on securing the IDE see Chapter 10 Working with Security in the Application Server User’s Guide.

The ArchestrA IDE also provides a revision history that tracks the life cycle activities of ArchestrA Objects, such as object creation, check in/check out, deployment, and import/export. When objects are checked back in to the Galaxy after making changes, a dialog box prompts the user to enter comments about changes you made. It is good policy to enforce the use of this feature in regulated environments.

Figure 13: ArchestrA IDE Check In Comment Entry

A log of all changes and comments is available from the object properties menu. An example log is shown below.

Figure 14: ArchestrA Object Change Log
4.1.2 Signature Manifestation - 11.50

21 CFR Part 11:
“(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).”

4.1.2.1 Signatures for Alarms and Events

The InTouch Distributed Alarm system includes the Alarm DB Logger utility that logs alarms and events to the alarm database. Alarm and event records are generated by the system and the signature is linked to a specific event. When an entire alarm or event row is retrieved, the signature is linked.

InTouch generated event records include the operator and a comment which is the Alarm Comment field of the InTouch tag. InTouch verification events can be handled with scripts that utilize the InvisibleVerifyCredentials() function.

All ArchestrA UDAs generate events. The ArchestrA generated event records include the operator and a comment. The operator column can be forced by setting a UDA to either Operate, Secured Write or Verified Write access. The comment column is the object description, all UDAs in an object will have the same comment therefore each event should be its own object. Boolean events can take advantage of the Boolean label extension for the UDA, which will be logged in the Value String column of the event database. Verified Write events will show both the done by and checked by operator in the OperatorName column.

When an InTouch alarm provider (e.g. InTouch or ArchestrA) is configured to use either operating system or ArchestrA authentication and an alarm occurs, the alarm record contains the full name of the operator in the Operator Full Name column, assuming the operator is logged on along with the time and date and event details. For example if a user is registered in the PLANT_FLOOR domain with a user ID of JohnS and a full name of John Smith, the Operator Full Name column contains John Smith. If the alarm is subsequently acknowledged, and the node performing the acknowledgement is set to use operating system or ArchestrA security, the alarm record contains the full name of the acknowledgement operator. Otherwise, the alarm record contains a computer name concatenated with whatever is in the $Operator tag.

Applications deployed in an FDA regulated environment should use OS security. InTouch applications that are ArchestrA based should use ArchestrA security and ArchestrA should use OS group or OS user security.

For information Wonderware alarms and events and logging see the InTouch HMI Alarms and Events Guide and “Working with Alarms and Events” in Chapter 8 of the Application Server User’s Guide.

4.1.2.2 Other Signatures

Wonderware products can be configured to produce other electronic signatures with the use of scripting and ArchestrA objects. The compliance of these records is up to the developer and should be verified during the testing and qualification phases of a project.

4.1.3 Signature/Record Linking - 11.70

21 CFR Part 11:
“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.”

4.1.3.1 Signatures for Alarms and Events

The InTouch Distributed Alarm system includes the Alarm DB Logger utility that logs alarms and events to the alarm database. Alarm and event records are generated by the system and include user name, time and date and all other event details.
4.2 Electronic Signatures - Subpart C

4.2.1 General Requirements - 11.100

4.2.1.1 Signature Uniqueness - 11.100 (a)

21 CFR Part 11:
“(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.”

FDA-audited industries should use the OS User Based or OS Group Based Security model for best results. Both OS Security models use Windows operating system authentication. This permits user name and password management, outside InTouch, directly in the Windows operating system environment. By using OS Security you benefit from the standard Windows functions for password aging, logon maximum trial, user name uniqueness and more.

It is not recommended to use local OS Groups as Roles, as that requires each node within a Galaxy to have the same OS Users, Groups, and user-group mappings to get the same level of access to the user at each node. Defining users on individual nodes creates a possibility of the same user name being assigned to different users. For example, if user name jdoe was used on a node for John Doe and jdoe was used on a different node for Jane Doe, within the same system, alarm or event records would not be able to distinguish between the users. Managing users in a single location and authenticating by connecting to that location eliminates the potential for multiple users having the same user name, which in turn ensures signature uniqueness.

4.2.2 Components and Controls - 11.200

4.2.2.1 Non-Biometric Signatures - 11.200 (a)

21 CFR Part 11:
“(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.
   (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.”

Systems should be set up to require user ID and password entry to authenticate users. Logging the authentication event or logon can then act as the first signing as all electronic signature components (ID, password) are required for logon and the user name of the logged in user can be recorded as part of the logon event.

Subsequent signature events (e.g. alarm limit change, alarm acknowledgement) can also include the user name to indicate the signing of the event. The user ID and password combination is not required to complete the signing while this same user is logged in as the duration of any logon for a user is a single, continuous period of controlled access.

If a user logs out manually, is logged out by another user logging in (e.g. to perform a checked-by function), or is inactive and logged out automatically by the system, the continuous period of controlled access ends. Any signatures would then require a new user to be logged in, which requires all electronic signature components (ID, password).

InTouch WindowViewer can be configured to automatically log off an inactive operator from an InTouch application. An operator must log on again after being logged off for inactivity. Setting an automatic inactivity log off period prevents unauthorized access to your InTouch application when operators leave their workstations unattended. Inactivity time periods should be evaluated for each system and vary according to the unique attributes and environment in which each system is operated.
Figure 15: InTouch WindowViewer Inactivity Configuration

For more information on using the WindowViewer inactivity features see the InTouch Security Features section in Chapter 5 Securing InTouch of the HMI Application Management and Extension Guide.

4.2.3 Controls for Identification Codes & Passwords – 11.300

4.2.3.1 ID & Password Uniqueness - 11.300 (a)

21 CFR Part 11:
“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.”

This requirement is addressed by the content in 4.2.1.1 Signature Uniqueness - 11.100 (a).

4.2.3.2 Password Changes - 11.300 (b)

21 CFR Part 11:
“(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).”

FDA-audited industries should use the OS User Based or OS Group Based Security model for best results. Both OS Security models use Windows operating system authentication. This permits user name and password management, outside InTouch, directly in the Windows operating system environment. By using OS Security you benefit from the standard Windows functions for password aging, logon maximum trial, user name uniqueness and more.

4.2.3.3 Transaction Safeguards - 11.300 (d)

21 CFR Part 11:
“(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.”

System events can be created to document failed logon attempts in the event someone attempts to logon as a different user. There is no technological control to prevent unauthorized use of IDs or passwords if those ID and password combinations are compromised or known to more than the individual assigned a specific ID and password combination.
5. Other Technical Products

Additional Wonderware products incorporate features and functionality designed to facilitate the development of applications for use in FDA regulated industries.

While it is outside the scope if this document to document best practices for 21 CFR Part 11 for these additional products, below are summary descriptions of relevant products and their capabilities relevant to regulated industries.

**Wonderware InBatch** - Wonderware InBatch software provides a powerful solution for effectively managing flexible batching processes found in regulated industries. Consistent with the ISA S88 industry standard, InBatch software offers comprehensive batch execution, equipment allocation, material genealogy, stringent security, and web-based reporting capabilities. Customers can improve Compliance & Governance through complete electronic system records for ‘as planned’ and ‘as executed’ information, including full Electronic Batch Records (EBR) in according with requirements found in FDA CFR 21, Part 11 regulations.
Wonderware Operations & Performance Software - provides a configurable and highly scalable Manufacturing Execution Software System (MES) solution that is integrated with Wonderware’s ArchestrA based System Platform and InTouch HMI for unsurpassed connectivity and flexibility and can be applied to essentially any manufacturing or process industry. Customers gain accurate equipment setup according to site specific product specifications; central administration of process and product parameters; consistent interpretation of operating guidelines and procedures – all with complete electronic ‘As-Built’ historical records for documentation of products and processes.

QI Analyst - Wonderware QI Analyst provides powerful Statistical Process Control (SPC) capabilities that can be leveraged in nearly any enterprise, with support for data entry, real-time and historical charting and statistical calculations, and real-time alarms. QI Analyst charts and objects can be used within an ActiveX container, and can be part of a validated system. QI Analyst also tracks all data-related changes, additions and deletions and tracks configuration activities that affect data integrity.
6. About The Co-Author

TSD, an Optimization Company (http://www.optimation.us), is a turnkey control and information system integrator providing control systems, batching systems, information systems, electrical design and installation, mechanical design and installation, and validation services. TSD, an Optimization Company, focuses on the Life Science industries and has years of experience providing systems that require validation and 21 CFR Part 11 compliance. TSD, an Optimization Company, has been recognized by Wonderware as an Endorsed System Integrator meeting the high level of technical competency required by the program and has delivered validated Wonderware systems including Operations and Performance Software.

7. References

1 21 CFR Part 11, Subpart A, section 11.1 (b)
2 Complying with 21 CFR Part 11, Electronic Records and Electronic Signatures, Part 2