



Wizcon® Supervisor™

The complete Internet-based solution for control and information

Wizcon 9.1.5

FDA 21 CFR Part 11 Compliance Statement

February 2006



Wizcon Systems SAS
Parc Technologique de Lyon
12 allée Irène Joliot-Curie
F-69791 Saint-Priest Cedex
France
tel +33 (0)4 72 47 98 98
fax +33 (0)4 72 47 98 99

Wizcon Systems BV
Concordiaweg 149-151
Postbus 351
NL-4200 AJ Gorinchem
Nederland
tel +31 (0)183 646 303
fax +31 (0)183 621 601

Wizcon Systems Ltd
The Gate Hotel, Scotland Gate
Northumberland
NE62 5SS
UK
tel +44 (0)845 606-6120
fax +44 (0)845 606-6121

www.wizcon.com
<http://support.wizcon.com>



Wizcon Systems

FDA 21 CFR Part 11 Compliance Statement

For Wizcon Supervisor 9.1





with Service Pack 1

Rev 5.0, January 2006

(Wizcon 9.1.5 - FDA 21 CFR Part 11 compliance.doc)



Approvals

Revision	Date	Written by	Reviewed by	Approved by	
5.0	31/01/06	Service Engineer  Fabien Mugnier	R&D Manager  Stuart Solloway	Technical Director  Philippe Grosjean	Marketing Director  Emmanuel Vitrac

Modification History

Version No.	Date	Change Details	No. Pages
0.1	Sept. 2003	Initial draft	18
0.2	Sept. 2003	Internal review	18
1.0	Oct. 2003	Release	19
2.0	Aug. 2004	Update for Version 8.3	19
2.1	Sept. 2004	Minor changes	19
3.0	Jan. 2005	Update for Version 9.0	21
4.0	July 2005	Update for Version 9.1	22
4.1	Oct. 2005	Minor changes in section 2	24
5.0	Jan. 2006	Update and review for Version 9.1 SP1	25
5.1	Feb. 2006	Update and review for Version 9.1.5 + enhanced layout	25

Index

Wizcon 9.1.5 position

Introduction to Wizcon's User Management concept.....	7
Implementation of the Access Rights in a project.....	9
Implementation of the Access Rights on Microsoft and Web level.....	12

FDA 21 CFR 11 - Subpart A

General Provisions	13
Sec. 11.1 Scope.....	13
Sec. 11.2 Implementation.....	14
Sec. 11.3 Definitions.....	15

FDA 21 CFR 11 - Subpart B

Electronic Records	16
Sec. 11.10 Controls for closed systems.....	16
Sec. 11.30 Controls for open systems.....	20
Sec. 11.50 Signature manifestations.....	21
Sec. 11.70 Signature/record linking.....	22

FDA 21 CFR 11 - Subpart C

Electronic Signatures	23
Sec. 11.100 General requirements.....	23
Sec. 11.200 Electronic signature components and controls.....	24
Sec. 11.300 Controls for identification codes/passwords.....	25

Purpose

This document describes the Wizcon for Windows and Internet 9.1.5 compliance with the US Food and Drugs Administration's Code of Federal Regulations, chapter 21, part 11 (aka FDA 21 CFR Part 11).

All text in *italics* is excerpted from the official FDA documentation.

Wizcon is a software suite providing a full set of tools to develop and deploy applications for Web-based Supervision, Control and Data Acquisition (SCADA) functionality as well as PC-Based Control operations. The design and development of the application and its compliance with the initial requirements or any sort of regulations remains the responsibility of the application developer and does not transfer to Wizcon Systems.

FDA compliance embraces complete systems including hardware, software, documentation, files & user management, user's rules of conduct, company security standards etc. Given that Wizcon is only one element in this system, Wizcon Systems (or any other SCADA software provider) cannot solely guarantee compliance; this is dependent upon the environment in which it is deployed.

However, Wizcon Systems guarantees that, providing the application is developed, deployed and used according to its own written guidelines, it will not in itself create any breaches of FDA compliance.

**TITLE 21
FOOD AND DRUGS**

**CHAPTER I
FOOD AND DRUG ADMINISTRATION,
DEPARTMENT OF HEALTH AND HUMAN SERVICES**

**PART 11
GENERAL PROVISION
ELECTRONIC RECORDS
ELECTRONIC SIGNATURES**

Contents:

Subpart A: General Provisions

- 11.1 Scope.
- 11.2 Implementation.
- 11.3 Definitions.

Subpart B: Electronic Records

- 11.10 Controls for closed systems.
- 11.30 Controls for open systems.
- 11.50 Signature manifestations.
- 11.70 Signature/record linking.

Subpart C: Electronic Signatures

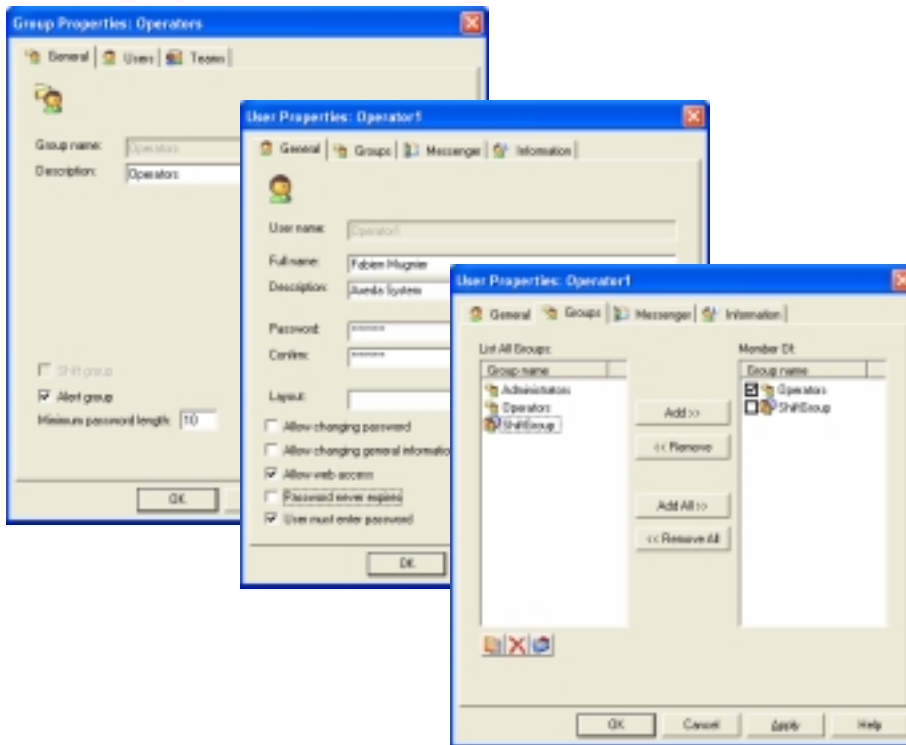
- 11.100 General requirements.
- 11.200 Electronic signature components and controls.
- 11.300 Controls for identification codes/passwords.

Wizcon 9.1.5 position

The following is the detailed list describing Wizcon for Windows and Internet 9.1.5 compliance with each point of the regulations.

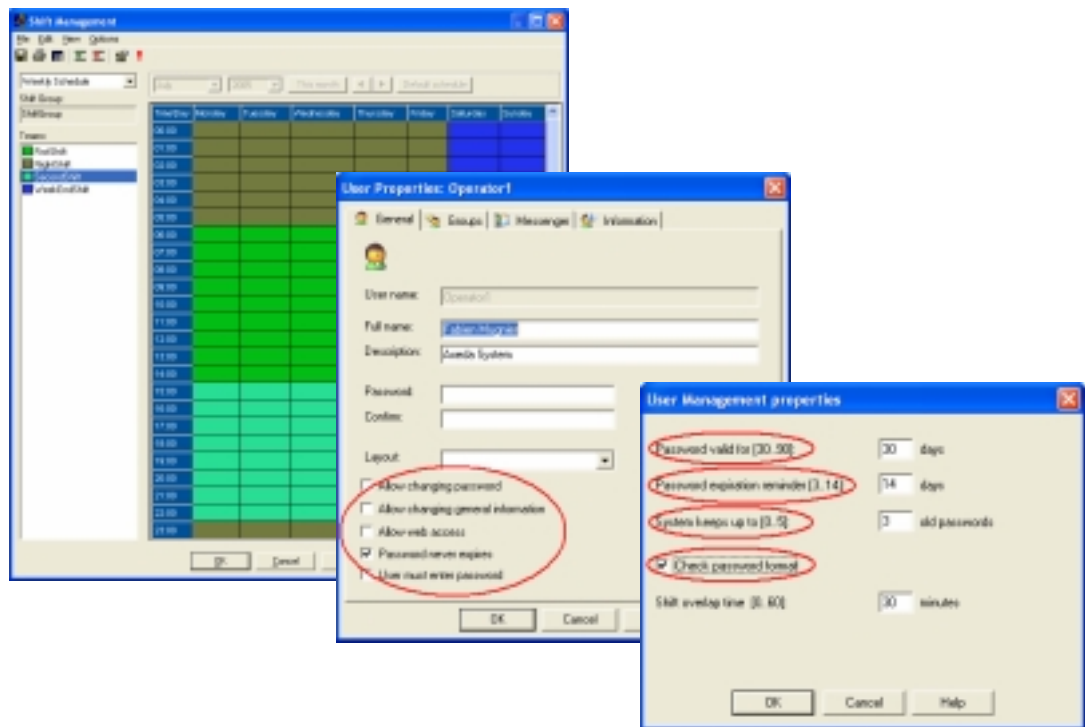
Introduction to Wizcon's User Management concept.

As required by FDA21 CFR11.200.1, Wizcon employs two distinct identification components such as a unique combination of password and login.



Furthermore, there are several levels of security access used to control access to Wizcon:

- Users must be created by an administrator
- Users can be requested to enter their own password upon first login.
- Users can be forced to change their password after a specific amount of time
- Rules on the content (a combination of letters, numbers and special symbols) and length of passwords can be applied.
- Users can be disallowed from using again their old passwords once their current password has expired.
- Upon 3 consecutive failed login attempts, an alarm is sent to all Wizcon systems on the network, thereby warning other users of potential security breaches. Actions to take upon such an alarm can be configured.
- A system of shift management can be used to control the times during which a user is allowed to login to the system.



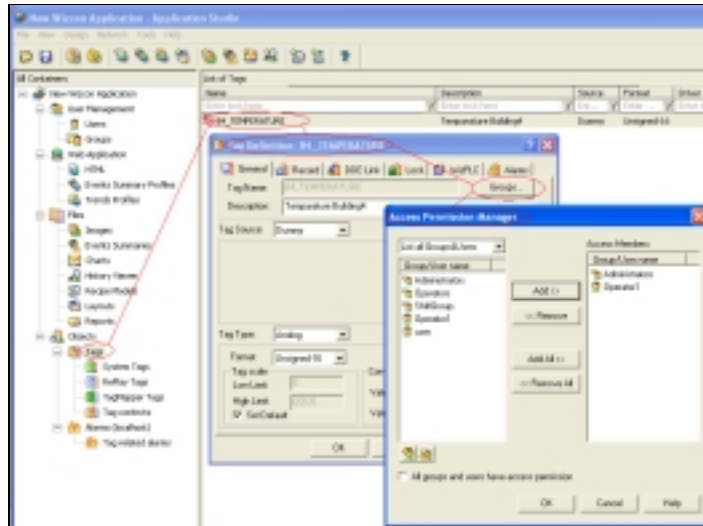
Implementation of the Access Rights in a project.

Access control to all alarms, tags, objects in images and menu items can be controlled via options available when defining the application. It is the responsibility of the application designer to ensure that the correct options are selected.

Access rights of a project can be defined for both Users and/or Groups of Users as described in the topics listed below.

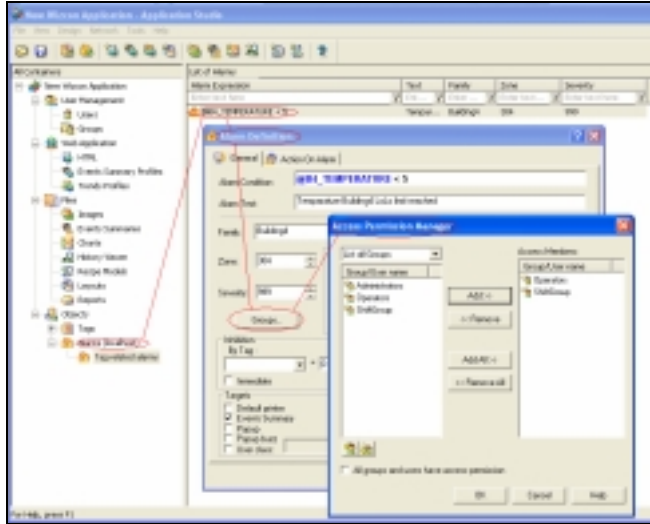
(a.) Access Rights for Tags

It is possible for each Tag to define Users and/or Groups of Users that are allowed to access this Tag. Below is an example of such a configuration where ONLY Administrators and Operator1 have the right to access this Tag.



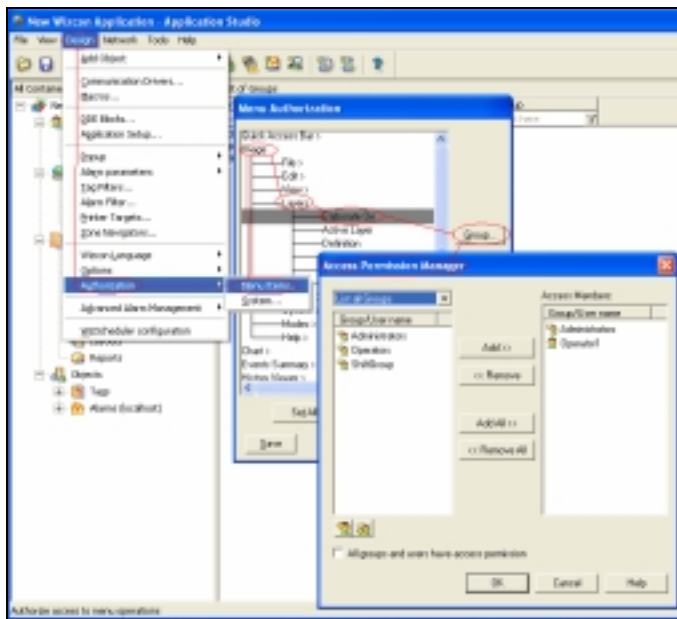
(b.) Access Rights for Alarms

It is possible for each defined Alarm to define Users and/or Groups of Users that are allowed to acknowledge this Alarm. Below is an example of such a configuration where ONLY Administrators and Operator1 have the right to acknowledge this Alarm.



(c.) Access Rights for Menus and Modules

Wizcon allows an extensive Access Rights configuration of the different modules and menu items. Below is an example of such a configuration where ONLY Administrators and Operator1 have the right to elaborate a Layer in an Image.

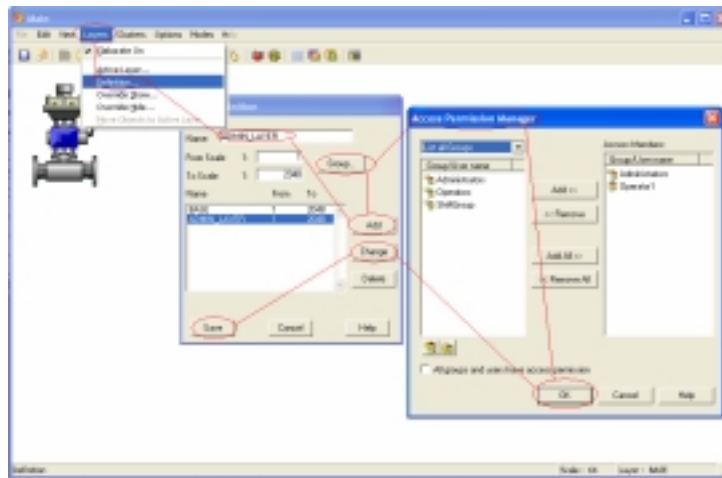


(d.) Access Rights for Objects in Images

Any object in an image can be defined to be accessible by specific Users and/or Groups of Users ONLY.

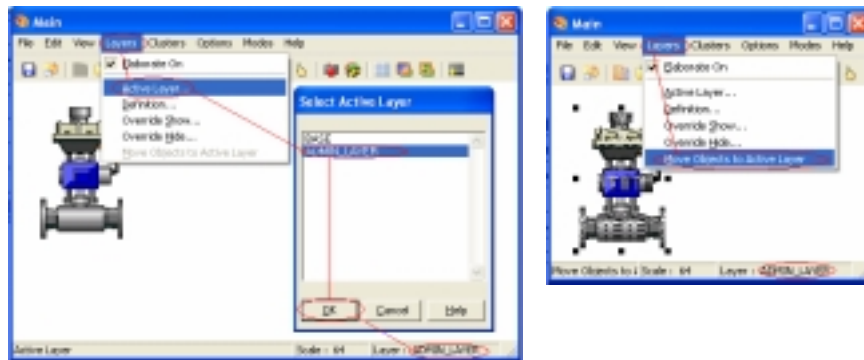
In order to set up such an environment, Wizcon provides access-right limited Layers on which the objects are placed. The default layer on an image is "BASE".

Below is an example where a new Layer "ADMIN_LAYER" is created and its access limited to Operator1 and Administrators ONLY.



To link an object to a specific layer, the layer must be first activated and the object then sent to this active layer.

Below is an example of a Valve sent to the previously created "ADMIN_LAYER"



Any logged operator who is either member of the "Administrators" Group or who is "Operator1" will see the previously configured layer and all of its objects.

Any logged operator that is not member of the "Administrators" Group nor is "Operator1" will not have access to the previously configured layer and will thus not see the objects on this layer.

Implementation of the Access Rights on Microsoft and Web level.

Wizcon's internal user management system can be linked to directly interact with the Windows security system, thereby controlling the level of access for a user to the actual PC. This allows, for instance, a user to have access only to Wizcon and no other programs that may be installed on the system.

The use of the above feature is optional, general access limitation can also be achieved using Microsoft's integrated User Management. If it is decided to implement the standard Microsoft user management mechanism for general access limitation, it remains the sole responsibility of the SI or customer's IT department to configure, manage and maintain these settings.

Please note that access to Wizcon is available via the intranet or internet using a standard web browser such as Internet Explorer. The same system of User Management as defined in Wizcon applies to any operator connecting thru a Web Client.

Wizcon Systems is not responsible for any security breach associated the Operating System or with the browser itself.

Implementation of adequate Firewalls, Antivirus and Networks are under the responsibility of the System Integrator or End user.

FDA 21 CFR 11 - Subpart A
General Provisions

Sec. 11.1 Scope.

- (a.) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.*
- (b.) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.*
- (c.) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.*
- (d.) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with Sec. 11.2, unless paper records are specifically required.*
- (e.) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.*
- (f.) This part does not apply to records required to be established or maintained by Sec. 1.326 through 1.368 of this chapter. Records that satisfy the requirements of part 1, subpart J of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.*

Sec. 11.2 Implementation.

- (a.) *For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.*
- (b.) *For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:*
- (1.) *The requirements of this part are met; and*
 - (2.) *The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.*

Sec. 11.3 Definitions.

- (a.) *The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.*
- (b.) *The following definitions of terms also apply to this part:*
- (1.) *Act means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).*
 - (2.) *Agency means the Food and Drug Administration.*
 - (3.) *Biometrics means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.*
 - (4.) *Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.*
 - (5.) *Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.*
 - (6.) *Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.*
 - (7.) *Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.*
 - (8.) *Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.*
 - (9.) *Open system means 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.*

FDA 21 CFR 11 - Subpart B
Electronic Records

Sec. 11.10 Controls for closed systems.

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:

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

Wizcon Systems' compliance: Wizcon Systems provides all tools for generation, development and maintenance of HMI (Human Machine Interface) projects. The design and construction of any project by use of Wizcon Systems' products as well as the verification of its compliance with the FDA requirements and its final validation remain the sole responsibility of the project designer, systems integrator and of the customer.

(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.

Wizcon Systems' compliance: Wizcon provides historical data points and historical alarm records in "standard database" format as well as in proprietary binary format.

- As "standard database", any ODBC compliant relational Database is supported.
- Alarm History data is stored in ALddmmyy.CDX (index) and ALddmmyy.CDX *.DBF (daily records) files.
- Tag History is stored in GTddmmyy.IDT (index), GTddmmyy.DAT (analog and digital daily records) and GTddmmyy.STR (string daily records) files.

These records can be viewed through standard viewers included in Wizcon Systems' HMI or through specific viewers via SQLRequests to the ODBC compliant relational Database.

Printing capabilities to provide human readable outputs are also included in Wizcon Systems' HMI.

(c.) *Protection of records to enable their accurate and ready retrieval throughout the records retention period.*

Wizcon Systems' compliance: Wizcon historical data are stored in proprietary format to avoid alteration and falsification.

However it remains the sole responsibility of the user to protect those files from being deleted, moved, and renamed or from any other actions which could harm the stored data.

Wizcon Systems recommends taking advantage of Microsoft's integrated User Management to limit access rights to these files.

(d.) *Limiting system access to authorized individuals.*

Wizcon Systems' compliance: Wizcon provides an advanced user management defining access rights to the project as described in the Chapter 1 of this document.

As required by FDA21 CFR11.200.1, Wizcon employs two distinct identification components such as a unique combination of password and login.

Regarding general access limitation to the Operating System, Wizcon also provides an advanced user management which directly interacts with Microsoft Windows security mechanism thus enabling the use of the HMI project ONLY. The use of the above feature is optional, general access limitation can also be achieved using Microsoft's integrated User Management. If it is decided to implement the standard Microsoft user management mechanism for general access limitation it remains the sole responsibility of the customer's IT department to configure, manage and maintain these settings.

(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.*

Wizcon Systems' compliance: When using Wizcon's proprietary coded format, there is no way to alter, falsify or delete a record of the historical data while Wizcon is running. However, it remains the responsibility of the customer to protect those files from being corrupted, damaged, deleted, moved or renamed, or from any other actions which could harm the stored data.

In case of using, in parallel with the proprietary files generated by Wizcon, an external ODBC compliant relational Database it is the sole responsibility of the customer's IT department to manage this Database. In case of MSSQL and records not being encrypted for this type of database, Wizcon Systems recommends activating the MSSQL Audit Trail feature in order to trace any manual changes to the records.

All user operations in the HMI such as changing a value via trigger, locking the value of a tag, going to a zone in the image, running a macro or logging in or out, are tracked by Wizcon's audit trail. All operations performed on alarms are also stored within the alarm historical file, with the user identification in term of action (acknowledgement, force end...).

(f.) *Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.*

Wizcon Systems' compliance: Enforcing permitted sequencing of steps and events, as appropriate, can be achieved by implementing sequential macros, actions on events and by designing steps as Image jumps. It remains the sole responsibility of the customer using these various methods to design its application in order to provide the appropriate operational systems checks.

(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.*

Wizcon Systems' compliance: Wizcon provides an advanced user management as described in the Chapter 1 of this document, defining access rights to the project modules (History viewers, menus, images, actions, Alarms...).

As required by FDA21 CFR11.200.1, Wizcon employs two distinct identification components such as a unique combination of password and login.

(h.) *Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.*

Wizcon Systems' compliance: In addition to the "normal" user login and password required, some installations require specific limitations for terminal. In practice, there can be a limitation when using a Web Client in terms of terminals that are allowed to access the system.

The simplest way to implement this limitation is to use a firewall listing the IP or MAC addresses of the allowed terminals and their actions. It remains the sole responsibility of the customer to chose, configure, manage and maintain these firewalls.

(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.*

Wizcon Systems' compliance: Wizcon's embedded user management consists of Users that are assigned to User Groups as described in the Chapter 1 of this document. Generally, access rights in projects are defined at a User Group level.

It remains the sole responsibility of the customer to verify that the users configured as being member of a User Group will have the education, training, and experience that corresponds to the tasks assigned to this User Group.

(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.*

Wizcon Systems' compliance: It is the sole responsibility of the customer to establish and maintain the adherence to such written policies.

(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.*

Wizcon Systems' compliance: The customer/systems integrator who has developed an application using Wizcon is responsible for writing its own documentation and maintaining it.

Sec. 11.30 Controls for open systems.

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in Sec. 11.10, as appropriate and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

Wizcon Systems' compliance: Wizcon is designed for CREATION and VIEWING of electronic records only.

MODIFICATION, MAINTENANCE and TRANSMISSION of such records are not part of the scope of Wizcon.

The establishment of written procedures and controls to ensure the authenticity, integrity and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt remains the sole responsibility of the customer.

"Operator driven electrical records" such as reports will be generated by Wizcon including the signature of the Operator liable for the document.

Sec. 11.50 Signature manifestations.

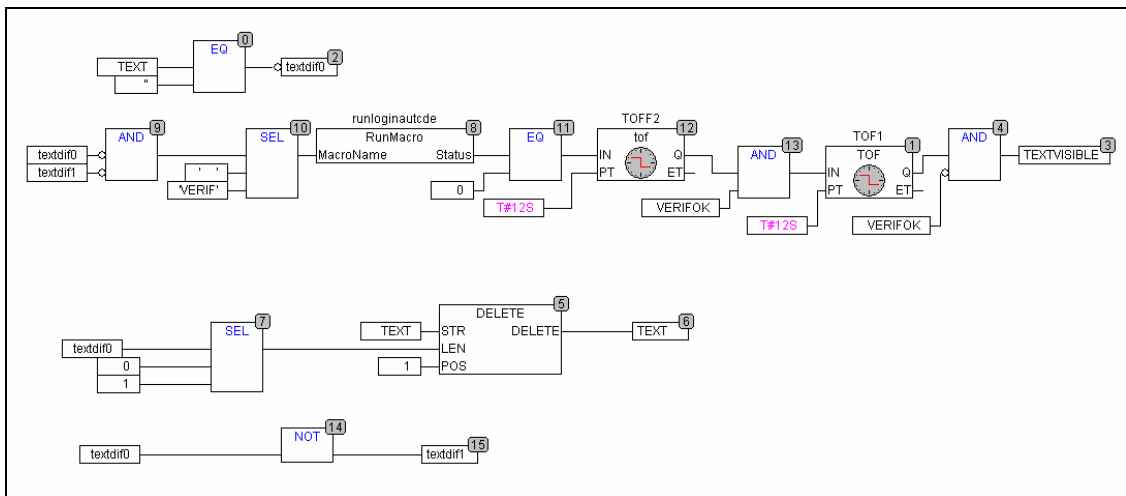
(a.) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

- (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.

Wizcon Systems’ compliance: Signed electronic records such as events and alarms recorded in archives files by Wizcon are written with the name of the user who has acknowledged the event or alarm with the date and time stamp of the acknowledgment. In addition, Wizcon is providing an audit trail to record the time stamped actions performed by the operator.

To include a meaning or any other comment related to this action, a WizPLC program can be implemented to force the operator to enter his signature along with a comment before being able to perform the action.

Below is an example of such a WizPLC program:



(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).*

Wizcon Systems' compliance: Wizcon includes viewers that allow any signed electronic record (such as the signed record of an alarm acknowledgement or a signed record of an action in the Audit Trail) that will be part of a human readable document or display containing the items specified under (a)(1), (a)(2), and (a)(3).

It is the project designer's responsibility to configure the standard viewers (Event Summary, Audit Trail...) in Wizcon to include these items.

Sec. 11.70 Signature/record linking.

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.

Wizcon Systems' compliance: All electronic signatures and their respective records are stored either in proprietary formats to Wizcon or in external, ODBC compliant, relational databases.

The definition of access rights to the possible relational databases and their maintenance (backups) remains the sole responsibility of the customer.

FDA 21 CFR 11 - Subpart C

Electronic Signatures

Sec. 11.100 General requirements.

(a.) *Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.*

Wizcon Systems' compliance: All electronic signatures are composed of a unique set of login and password.

It is the customer's sole responsibility not to give an already used set of login/password to another or different operators.

(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.*

Wizcon Systems' compliance: The verification of the operator's identity before establishment, assignment or certification of an electronic signature (login/password) is the sole responsibility of the customer.

(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.*

Wizcon Systems' compliance: The certification to the agency by the person using electronic signature that this signature (login/password) are intended to be a legally binding equivalent to traditional handwritten signatures remains under the direct responsibility of the customer.

(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.*

Wizcon Systems' compliance: The submission in paper form of the certification to the Office of Regional Operations remains under the direct responsibility of the customer.

(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.*

Wizcon Systems' compliance: Providing additional certification or testimony upon agency request remains under the direct responsibility of the customer.

Sec. 11.200 Electronic signature components and controls.

(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.*

Wizcon Systems' compliance: Wizcon employs two distinct identification components such as a unique combination of password and login.

(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.*

Wizcon Systems' compliance: In Wizcon, the first and all subsequent signings are always composed by the two identification components (login/password).

(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.*

Wizcon Systems' compliance: In Wizcon, the first and all subsequent signings are always composed by the two identification components (login/password).

(2.) *Be used only by their genuine owners; and*

Wizcon Systems' compliance: Verification and certification that a unique combination of identification components is not used by different individuals is the sole responsibility of the customer.

(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.*

Wizcon Systems' compliance: It is recommended that the customer shall prohibit the use of an individual's electronic signature by anyone other than its genuine owner.

(b.) *Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.*

Wizcon Systems' compliance: Wizcon could be configured to integrate the Microsoft Windows user management mechanism which could include the support of electronic signatures based on biometrics but it is the responsibility of the application integrator to design, develop and validate the system.

Sec. 11.300 Controls for identification codes/passwords.

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.*
Wizcon Systems' compliance: Wizcon's user management mechanism prohibits the coexistence of identical sets of signature identification components.
- (b.) *Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).*
Wizcon Systems' compliance: Wizcon's user management mechanism includes a configurable password aging mechanism to ensure the periodical checking, recalling and revision of the identification code and password issuance.
- (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.*
Wizcon Systems' compliance: The implementation of such controls as to remove from the system or republish a combination of signature components that has become compromised remains the sole responsibility of the customer.
- (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.*
Wizcon Systems' compliance: Wizcon generates a system wide alarm upon the third failed login attempt. The configuration of an urgent reporting (par fax, E-mail, SMS...) linked to such an event and its possible subsequent actions (logout, locking of the station...) remains the sole responsibility of the project designer.
- (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.*
Wizcon Systems' compliance: Although the use of token or cards as signature components are not natively supported by Wizcon, such integration can be achieved by the use of external card readers for example. Initial and periodic testing plan for these components remains the sole responsibility of the customer.