INDUSTRIAL AUTOMATION SOFTWARE
progea

Movicon® 11
MONITORING VISION AND CONTROL

Designed for
☑ FDA
21CFR Part 11

How to get your Movicon 11 project FDA 21 CFR Part 11 ready

Document:	**RAC-4105**
Released:	**29-04-2005**
Updated:	**06-03-2012**
Rel. Movicon:	**11.3 or later**

Summary

Document's Aim

To briefly explain the DFA CFR21 Part 11 regulations. To describe the procedures and actions to take along with helpful advice to make the applied project, based on the Movicon 11 SCADA platform, perform in conformance with these regulations.

ⓘ

ⓘ *This document has been written by Progea Srl to inform Movicon Developers about its concepts and the best way to apply it with digital data recording functions and in the "electronic signature" application as required by the FDA regulations. This document has no legal value and is not liable in any way to Progea: it is the client's responsibility to verify that they have developed the application in compliance with the above mentioned regulations along with any updates that may have been made.*

Introduction

The aim of the CFR21 Part 11 regulations, written up by the FDA (Food & Drug Administration), is to obtain a legal equivalence between electronic documents (digital records and electronic signatures) and traditional paper documents. This has evolved due to the increasingly frequent use of automatic systems in managing production processes in systems that operate under FDA approval. In order that automation and control systems are realised in conformance with the CFR21 Part 11 regulations it is necessary that all recorded data is made referable to the operator in charge (Electronic signature), furthermore certain regulations regarding any precautions must be adapted to safeguard against forgery and mishandling of electronically recorded data, or to allow easy identification of any misuses, whether intentionally or unintentionally, of electronic devices which generate electronic records. Many pharmaceutical industries have especially benefited from using electronic records where untold amounts of paper documentation, archived over many years of research, has been transferred into electronic records which not only has reduced space but also precious time in acquiring and reviewing important information before releasing medicine on the market for sale.

It is absolutely crucial that these types of industries have the devices with the right protection mechanisms to safeguard against any intentional or unintentional data errors in electronic format.

Electronic Records: All significant processed data on production quality and regularity must be permanently recorded and not tampered with on the processor. These documents, called records, must be prepared, dated and signed by a person and again dated and signed for approval by the production manager or whoever is in charge. These records must be stored for at least one year after the production batch's expiry date. The owner of the signature is held legally responsible for any errors that may occur. Electronic records may be composed with texts, graphics, data, tables or any other information in digital format which is created, edited, stored, filed, retrieved or distributed using a computer system.

Electronic Signature: An electronic signature is a combination of symbols that can be used, adopted or authorised by an individual as a legal equivalent of their own handwritten signature.

CONTROL SYSTEM REQUIREMENTS

The Control Systems must be capable of acquiring the status and behaviour of the process's variables in realtime. The date and the product batch number must be entered along with the electronic signature of the operator and an eventual signature of approval from the process manager in the section relating to the product batch's working period. These procedures must be carried out without the threat of causing errors and that signatures are always unique and referable to their owners. The records must be filed in a save place and stored for an adequate time period. They must also be protected against unauthorized access.

Security

There are usually **two reasons** why data is recorded in electronic format.

The first being when data always has to be printed and signed for approval (the so called Hybrid solution: paper and electronic). In this case the file is to be considered an electronic record: the main problem is to ensure that the file and its data contents are not substituted or modified before being printed, identified, dated and signed. However the electronic signature may not always be necessary when signed manually. Therefore, for example, it is necessary that the data format is uneditable and is individualized and automatically associated to a specific production batch or line. Furthermore the original data file must be archived. This reason can be conclude by saying that a hand written signature does not necessarily give authority to an electronic record inadequately protected.

The second reason is to keep records filed in electronic format. Apart from guaranteeing that the file and its data contents cannot be substituted or modified and need a signature of approval, the electronic signature is also required. The data file should include information on the production batch it refers to and the name of the person who approved this data, being the person registered as logged on when data approval took place. All the file's contents should then be protected from any unauthorized modifications.

The electronic signature

The electronic signature can be created with a combination of at least two items such as an ID code and a password or a badge and a password etc., as required by the **CFR21 part 11**. The ID – password must be guaranteed that it is unique to that person with absolute certainty of identifying them. The ID code can be made public, meaning that it can be shown on screen. Since the password may not always be guaranteed as being unique to just one person, it is absolutely necessary that the ID code be original and personal to each user. These rules should be followed:

1. A set minimum password length
2. Change password periodically
3. Carry out procedures to avoid any attempts of meddling or unauthorized access
4. Record any attempts of unauthorized access
5. The system administrator must not know the password of other users even when assisting them when they have forgotten their password.
6. User Groups can share the same password only for reading data where the electronic signature is not required.

General Concepts for supporting these regulations

The concepts described below define how to use Movicon to develop applied projects with compatibility with the act and its regulations discussed in this document.

A list of the main concepts has been put together by Progea to give a clearer picture on the indications explained henceforth and which are based on the understanding that it remains the user's responsibility to ensure that the application, developed with Movicon, is compliant with these requirements.

Security

- The Movicon project must be **encrypted** (Movicon uses a 128 bit encoding) so that all the configurations and passwords used in the project are accessible from the outside.
- Movicon **guarantees unique user password entries** in the project. Each user is identified in the project with a UserID, Password, printable Description or Name (Electronic Signature). Movicon does not accept Users with the same electronic signature name (unique identity control) of another individual. The names must be made up with not less than 4 characters and not more than 64 characters.
- To guarantee data integrity and safeguard against any tampering of data, the Movicon application should be run as **Service of the Windows Operating Systems**. This will require identification of users registered in the system's domain according to the security requirements stipulated in order to access the operating system and its files. However, Windows Services may be differ according to the operating system being used as explained in the paragraphs below.
- Movicon supports **Windows XP/Vista/7 OS domain sharing** so that the user passwords, set up by the system administrator, can be used.
- Users who manage the recording of data by using the Data Loggers must take the right measures to prevent any unauthorized access, undesired modifications and tampering to database records. The **IMDB** archives (InMemory DB) allow users to manage **encrypted** historical log files or secure databases can be used, such as **Microsoft SQL Server or Oracle** with the appropriate administering of the Windows XP/Vista/7 operating system, which only permit the system administrator or developer access to records.
- To put an access limit on the developed application's functions and controls, the Movicon project must use the User Password Profile management correctly,

which involves the entering of a Password, UserID, User Name and Access Level. Movicon provides 1024 access levels and 16 areas.

- Users must manage their passwords with great care and integrity. New users, inserted by the administrator, can replace their password with a more personal one on their next Log On.
- All passwords can be set with an expiry time to make the user to issue a new password periodically, which will contribute to increasing system security.
- To fully comply with the regulations, the **Auto LogOff** (timeout of enabled access) must be appropriately used in the Movicon password management in order to prevent unauthorized access to the system after a certain period of user inactivity.
- To ensure validity and the correct entering of data, users must make sure that the Movicon operating stations are allocated in safe places and that they are accessible to authorized personnel only.
- The Movicon **AutoLogoff** function must be used in systems in continuous use.
- Movicon has tools and procedures that can be used for discouraging any unauthorized access attempts and are the same as those used in the Windows XP/Vista/7 operating system as required by the regulations. After the third failed attempt to access, Movicon will purposely take longer to respond to the re-entry of the password to discourage the intruder.
- Any further attempts to violate the system (Upon the third unauthorized Log On attempt) Movicon will display and record the event in the Historical Log in order to safeguard against and control any further system violations.

Digital Recording/Electronic Signatures

- Movicon returns the descriptive name of the registered user to identify and individualize the active operator.
- The applied program must be configured to record electronic signatures each time a digital recording is carried out (creating a record in the database) as required by the regulations. The user must execute LogOn in the project by linking two combined data (UserID and Password), and the electronic signature must be the genuine name of the user, the date, time and reason for the recording. The Movicon Data Logger allows the recording of all necessary data on the Database.
- For reasons of legal responsibility relating to the Electronic Recording, the operator must always be acknowledged every time data is recorded or when accessing the system. The User's ID is unique and belongs to that user only in Movicon and no other individuals are allowed the same ID.

- To satisfy the Electronic Recording requirements, the recording of events must be configured appropriately by using the IMDB archives (InMemory DB) where **crypted** historical log files can be managed or if **ODBC** archives, such as the **Microsoft SQL Server** or **Oracle**, secure databases must be used with the correct security management administered. Furthermore the user must configure applications to acquire and record electronic signatures on record of any operator undertaking actions. The user must also prevent any data from being lost by configuring the application to execute backups of all data recorded, or by using the Movicon redundancy functions. The user can also eventually configure the system so that it uses the Data Logger resource to record crypted data on IMDB or on relational ODBC database files. If needed, new data files can be created with prefixed timeframes (eg. Every 4, 8 or 24 hours) by using the Basic Script functions.

- The user can configure the system to copy recorded data in a safe and secure location by using procedures appropriately written with Basic Script codes. The Windows XP/Vista/7 OS security functions protect files and their data from any unauthorized access. When multiple files are created the user must control whether the right code is entered to prevent saturating free space on the hard disk where the oldest files may need to be deleted.

- The user may have to synchronize the system's time in real time or to that of another system's (Microsoft or third parties) so that recorded data relate to the true date and time, or they may have to manage data synchronization between Client and Server so recording becomes coherent. Synchronization of this type can be managed directly with the Windows XP/Vista/7 OS functions or with the Basic Script codes for third party products.

Validation and Documentation

- Some of the requirements stipulated in the regulations are not altogether implemented in software applications. These Part 11 requirements can be satisfied if the client validates their application to guarantee accuracy, reliability and security when recording data, as well as the capacity to prevent unauthorized editing, errors and data deletions. The Movicon users must validate their application in order to comply with the FDA act. The users can develop and/or execute the validation of programs and protocol themselves or delegate this task to others. The validation must follow a methodology established from system's life cycle (SLC).

- In order to meet the controls requested by the regulations in this act, the client must adopt adequate procedures to verify the identity of the individuals who have been assigned an electronic signature.

- The client must enter and set up the operator and their operating responsibilities executed under their electronic signature, to impede any forgeries or tampering of signatures or recordings, in compliance to the regulations of this act.

- The client must always be certain on the identity of the individual assigned an electronic signature. Furthermore the client is held responsible that the enrolled operator is fully aware of the regulations stipulated by the FDA agency and that they intend to use their electronic signature as a substitution and an equivalent of their own handwritten signature used on traditional paper and, when necessary, produce certification of their true identity, being legally binding to their handwritten signature, when under FDA inspection.
- The client is responsible for producing documentation on system use or on the application realized, on its distribution and updates, and also the details on personnel training. However, the client is not responsible for documentation on the platforms being used (Movicon, Windows).

Other

- All the data must be stored in a relational database, which fully meets the necessary security requirements (ie. IMDB crypted data, SQL Server or Ocracle with the relevant protection) and protected from any violation to or tampering of the security functions belonging to the Win2000/XP/Vista OS. Data must be filed and kept available for an adequate period of time according to the operating requirements.
- To further enforce the safeguard of data, project, images and recipes the user should use a third party software type, which can guarantee version maintenance and management (eg. Microsoft Source Safe can be used for controlling the versions).

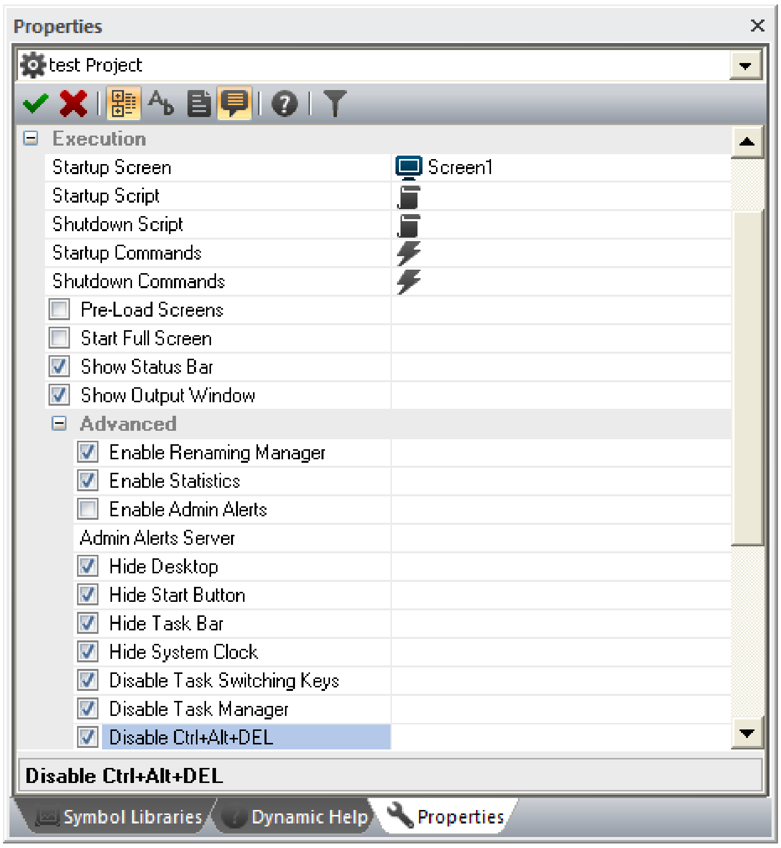
Configuration Techniques

To get a Movicon 11 project 21CFR Part 11 ready, you need to configure it appropriately so that it is compactable with the FDA validation criteria. The necessary measures to take in doing this are indicated below:

Security

- The project must be configured in its General Properties by selecting **"Cripted Project"** and **"Cripted Project Resources"**. In this case all the project's XML information can be accessed by using a 128 bit encoding. To prevent unauthorized system access, select all the project's **Execution Properties** which **deny Operating System and Desktop access**. The following can be denied:
    - Windows Desktop
    - The Start button form the Windows' Task bar
    - Windows Task Bar
    - Windows task Options
    - Windows Task Manager
    - Windows CTRL+ALT+DEL
    - **Warning! Commencing with Windows Vista/7 Microsoft has implemented securities which impede the "Ctrl+Alt+Del" combo keys and the Windows "Start" button from being disabled.**

- As an alternative, Movicon can be run as **"Service"** of the operating system, as described in more detail ahead. When Movicon is run as service, it does not manage the project's properties that deny operating system access and which are listed above.



Execution

Startup Screen	Screen1
Startup Script	
Shutdown Script	
Startup Commands	
Shutdown Commands	
□ Pre-Load Screens	
□ Start Full Screen	
☑ Show Status Bar	
☑ Show Output Window	

Advanced

☑ Enable Renaming Manager	
☑ Enable Statistics	
□ Enable Admin Alerts	
Admin Alerts Server	
☑ Hide Desktop	
☑ Hide Start Button	
☑ Hide Task Bar	
☑ Hide System Clock	
☑ Disable Task Switching Keys	
☑ Disable Task Manager	
☑ Disable Ctrl+Alt+DEL	

Disable Ctrl+Alt+DEL

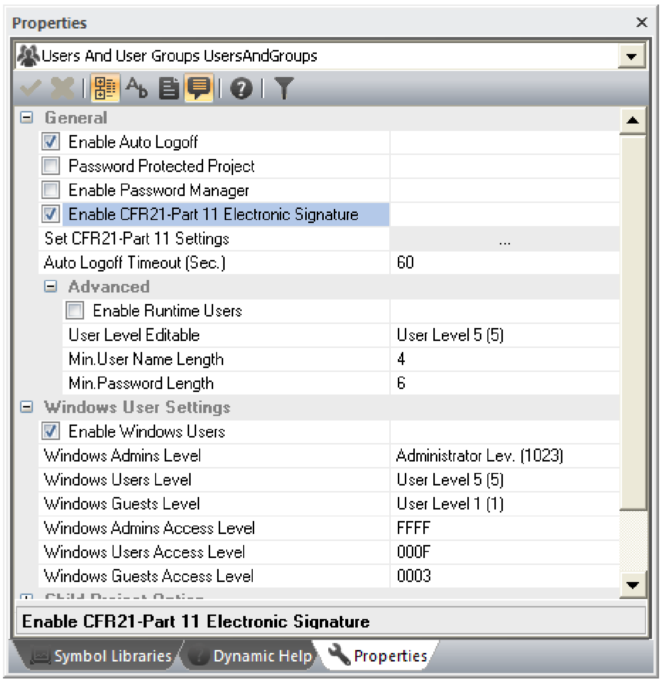
An illustration of the project's properties window

Important! Commencing with Windows Vista/7 the use of the graphical interface for Windows Services will no longer be supported. Windows Vista/7 has increase security by keeping the running of services and user applications in separate sessions. This not only increases system service security but also impedes the user from interacting with the service's user interface.

Running Movicon as Windows Vista/7 service will therefore exclude the use of the graphical interface. This problem can be avoided by creating a "Client" project which will be launched in the Windows user interface and communicate in network with the "Server" project launched as Service enabling use of the Server user interface remote control mode.

Passwords

- All the application commands that can be executed by operators to interact on the process must be protected by passwords.
- The password management must be enabled in the project's **User Passwords resource Properties**:
    - **Project Protected with Password**: the password will be requested only for entering in "Development" mode
    - **Enable Password Management**: the passwords will be activated according to the levels and access modalities to the preset commands.
    - **Enable Electronic Signature**: the unique user Description of the user whose name is to be used as an Electronic Signature will be managed.
    - **Auto Log Off**: determines the time (sec.) for automatically deactivating the active user after a period of inactivity.
    - **Minimum Length (user name and password)**: set for default at 4 and 6 characters respectively, as suggested by the regulations.
- Secondary parameters relating to the password management need to be set according to the general properties illustrated below.



Properties

Users And User Groups UsersAndGroups

General	
☑ Enable Auto Logoff	
□ Password Protected Project	
□ Enable Password Manager	
☑ Enable CFR21-Part 11 Electronic Signature	
Set CFR21-Part 11 Settings	...
Auto Logoff Timeout (Sec.)	60
Advanced	
□ Enable Runtime Users	
User Level Editable	User Level 5 (5)
Min.User Name Length	4
Min.Password Length	6
Windows User Settings	
☑ Enable Windows Users	
Windows Admins Level	Administrator Lev. (1023)
Windows Users Level	User Level 5 (5)
Windows Guests Level	User Level 1 (1)
Windows Admins Access Level	FFFF
Windows Users Access Level	000F
Windows Guests Access Level	0003
Child Project Option	

Enable CFR21-Part 11 Electronic Signature

The project's User Password Resource properties window.

Windows Security Synchronization

Movicon provides the possibility to share, in applied applications, users from the operating system domain or from a Windows XP/Vista/7 server.

Therefore, when activating the password management, the project will acknowledge and accept users inserted and activated from the domain of the installed operating or from a server station.

Movicon accepts mixed configurations, whether being users inserted on the project list, or users deriving from the XP/Vista/7 domain.

Users on the project list can be associated with a customized user level. Users deriving from a XP/Vista/7 *station domain can receive a customized user level when inserted on the user list, otherwise they will be associated the same password level specified for the group they belong to (Administrators, Users, Guests).*

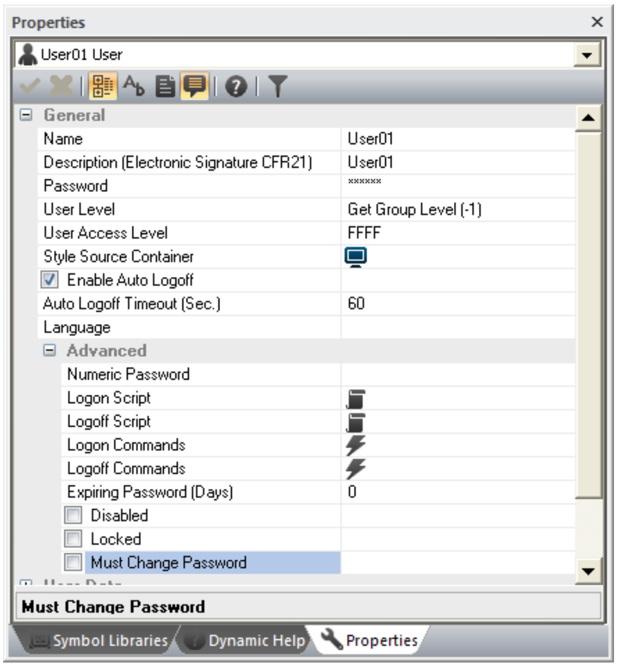
Different password levels can be assigned to domain users. This function is made available by adding users to the Movicon user list who have the same UserID configured in the primary domain controller. Password authentication and validity are carried out by the primary domain controller for those users configured in this way. For instance if a user with UserID = “guest” exists in the primary domain controller, a user can be configured with the same UserID, in this case “guest”, and the password can be left blank in the Movicon project’s user list. By doing this the user can be assigned the appropriated level desired. In runtime, the user’s name and password, which are inserted in the Movicon user authentication window for logging on, are validated by the primary domain controller. This permits expiry passwords to also be used for Windows users.

This feature is also valid for users configured directly in runtime with the Movicon edit users window.

User Passwords

- Each user or user group who has access to commands or process interaction, must be inserted and configured in the project appropriately.
- Users are inserted in the project’s **User Password Resource** where they can be configured in their properties. These properties include those which involve the requirements stipulated in the FDA act:
  - **Name (ID) and Password**. These are assigned to the user and are used for identification by the system.
  - **Electronic Signature**: This is a **unique** text which corresponds to the user’s electronic signature and is recorded as absolute user identification (the Electronic Signature management must be enabled in the **User Password Resource)**

- **Auto Log Off**: This can be specified singularly for each individual user.
- **Expiring Password**: The act stipulates that the user password expires after a certain preset time so that the user is obliged to change it periodically to increase system security.
- **Must Change Password**: For identification certainty this obliges the user to enter their own personal password on the next Log On so it is only known to themselves and no one else including the administrator who logged them on the first time.



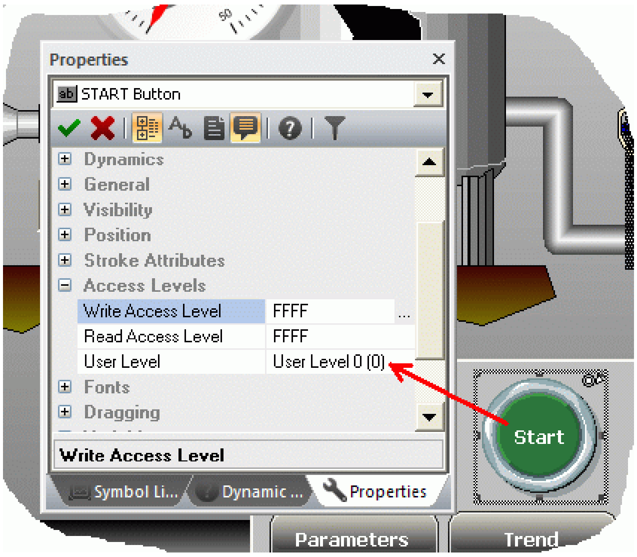
⊟ General	
Name	User01
Description (Electronic Signature CFR21)	User01
Password	******
User Level	Get Group Level (-1)
User Access Level	FFFF
Style Source Container	
☑ Enable Auto Logoff	
Auto Logoff Timeout (Sec.)	60
Language	
⊟ Advanced	
Numeric Password	
Logon Script	
Logoff Script	
Logon Commands	
Logoff Commands	
Expiring Password (Days)	0
☐ Disabled	
☐ Locked	
☐ Must Change Password	

Must Change Password

This is a user properties window.

Command Access

- Each command, change or setting influencing the process must be given protected access by requesting user identification.
- The **User Level** in a hierarchical scale structure must be set in the "Access Level" property of each object. The Levels in Movicon start from 1023 (reserved for the system administrator) to level 1 (the lowest operating level). The 1024 level is reserved for the programmer.
- The command objects can also be provided with a **Access Level (Area)** in read or write, permitting users to access commands not only on a hierarchy scale but also by area of competence.



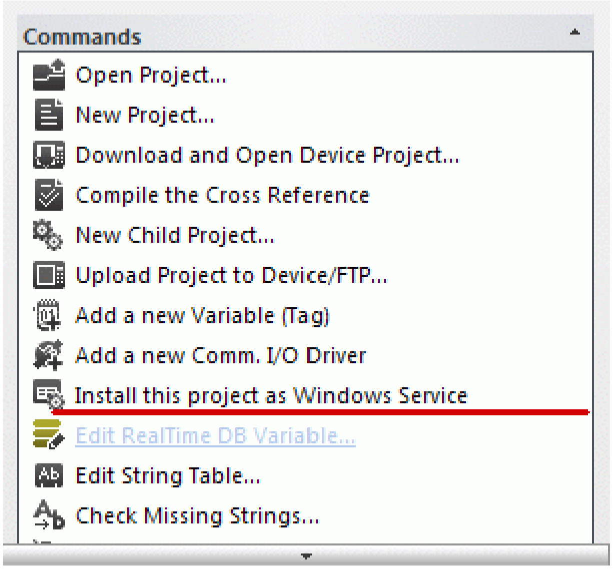
Write Access Level	FFFF
Read Access Level	FFFF
User Level	User Level 0 (0)

Write Access Level

Operating System Access

Movicon provide the possibility to block and deny operating system access. The follow two modalities can be used:

- **Lockout Windows access from Movicon:** to prevent unauthorized access in the system you need to select all the project's **Execution Properties which deny access to the Operating System and Desktop**. When Movicon is started up these will deny access to Windows according to the settings, which have been activated (described above).
    - **Warning! Commencing with Windows Vista/7 Microsoft has implemented securities which impede the "Ctrl+Alt+Del" combo keys and the Windows "Start" button from being disabled.**
- **Using Windows services**: you can configure the project to be installed as the operating system's **Service,** therefore it will be started up automatically before the Windows XP/Vista/7 operating System's Log On procedure. By doing this, as an alternative to the above indications, only the system administrator can access the operating system.


Commands
Open Project...
New Project...
Download and Open Device Project...
Compile the Cross Reference
New Child Project...
Upload Project to Device/FTP...
Add a new Variable (Tag)
Add a new Comm. I/O Driver
Install this project as Windows Service
Edit RealTime DB Variable...
Edit String Table...
Check Missing Strings...

This is the Project's control panel. The command, underlined in red, automatically installs the project as Service.

As explained above, the running of Windows Services differs depending on the operating system being used. Therefore particular attention must be paid to graphical interfaces for Windows Services using Windows Vista/7 operating systems where their use is no longer supported.

Biometric Systems

Using Biometric Systems is highly recommended in application validity according to the regulations.

In this case you need to choose the right recognition system among those available on the market that can be easily integrated into your application.

The most popular biometrics systems are ultimately those that use digital fingerprints. These systems are simple to use and integrate perfectly with operating systems and software applications.

Examples:

Progea has run tests on the Toca Fkey product (digital fingerprint scanner). This device can be plugged in to a USB port and has its own user profile management where the Movicon project users can be associated by using the appropriate VBA script module provided by Progea. This biometric system can be completely integrated into the project using the Movicon "User Password –Fingerprint" association.

- Movicon has also run tests on the Microsoft Fingerprint product, a simple and reasonably priced device that can be plugged into any USB port with Windows XP. This system runs its own software as service and provides files where users are inserted and recognised by their biometrics every time a password entry request is made. A tool, such as this one, does not require any project modifications or any particular interfacing or configuration. However, authentication of the operating system's users (Windows XP only) is only allowed when the PC users do not belong to a Domain.

Any type of biometrics recognition system can easily be used if the operating system has been predisposed to support one as described above, otherwise it can be integrated into the Movicon application by using the appropriate Basic Script interface.

Recording data (Audit Trail or Tracing)

Movicon provides the possibility to trace all the status changes of each variable which has significant relevance to or influence on the process: Usually all the set-point or process command changes need to be traced.

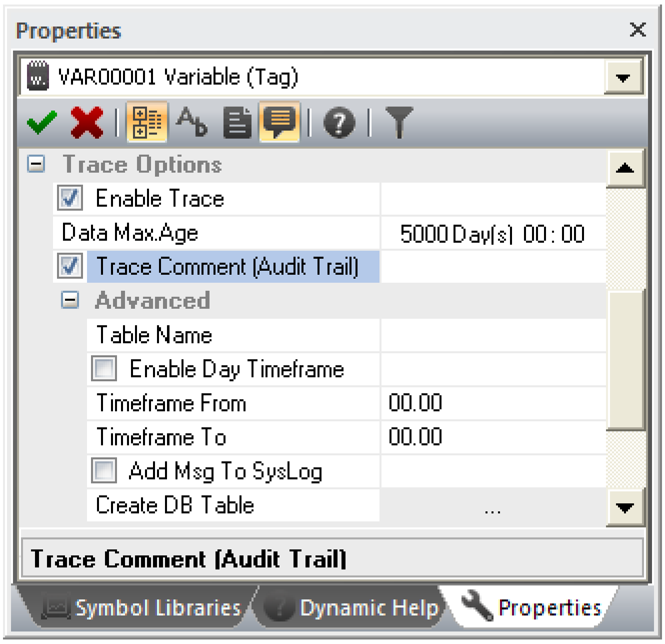
- Note the difference between the Trace and Data Logger files: The Trace records each data value change in the appropriate database along with all the relevant information, while the historical value recordings refer to the historical logging activity executed by the Data Logger resource.
-

In certain cases, it is sufficient enough to carry out the following procedures to sensitive data:

1. Request user identification before accessing to commando
2. Identify user and validate them (password management)
3. The user carries out the changes. The variable (Tag) is traced.
4. The value change is recorded in the appropriate Trace DB, reporting the date, the previous value, the current one and electronic signature.

All the historical information inherent to each change that took place in the process can be obtained from the appropriate Trace viewer so it can be easily traced back to what caused it.

The Tracing function is one of the properties belonging to each single Variable (Tag) and must be activated and configured by clicking on the **"Trace Options"** property in each Tag (variable).



Properties

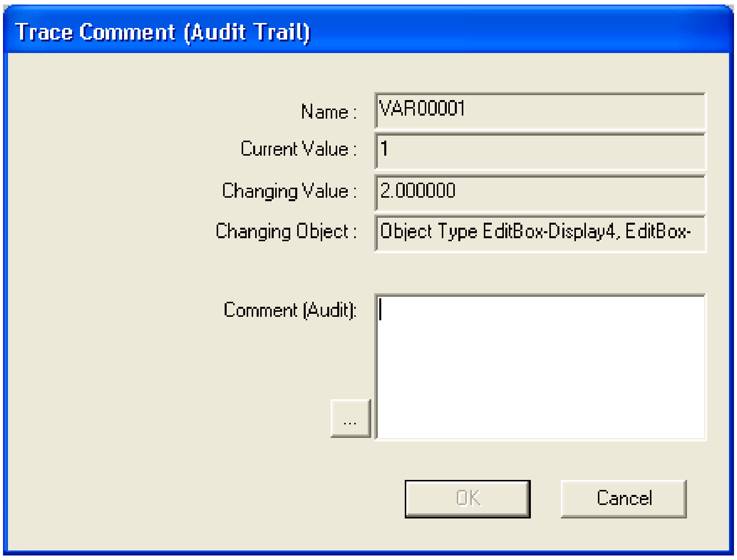
VAR00001 Variable (Tag)

⊟ Trace Options	
☑ Enable Trace	
Data Max.Age	5000 Day(s) 00 : 00
☑ Trace Comment (Audit Trail)	
⊟ Advanced	
Table Name	
□ Enable Day Timeframe	
Timeframe From	00.00
Timeframe To	00.00
□ Add Msg To SysLog	
Create DB Table	...

Trace Comment (Audit Trail)

Audit Trail

In many cases, before the user can proceed in making any process variable changes (eg. Set points), confirmation may be requested before the change can be put into action, together with a comment to explain the reason why this change has been made. (text string). In order to enter this comment the "Trace Comment" item needs to be ticked/checked in the Trace Property beforehand.



Trace Comment (Audit Trail)

Name : VAR00001
Current Value : 1
Changing Value : 2.000000
Changing Object : Object Type EditBox-Display4, EditBox-
Comment (Audit):

Movicon will display the window shown above after each manual Tag change occurs and authenticated by the user, indicating the change and requesting the user to state the reason this change was made. The comment inserted by the user is recorded:

- In the 'ActionCol' column of the Tracing DB table referring to variable which was changed.
- If the 'Add Msg to SysLog' check box has been checked, the event and the comment are also recorded in the main historical Log DB, in the 'DescCol' of the Historical Log's 'SysMsgs' table.
- *Note: When the 'Trace Comment' window is open on screen, the variable's value will freeze. Any other process, such as the drivers, the IL logic, basic scripts, will not be able to change it.*

Audit Trail with Process Manager Validation

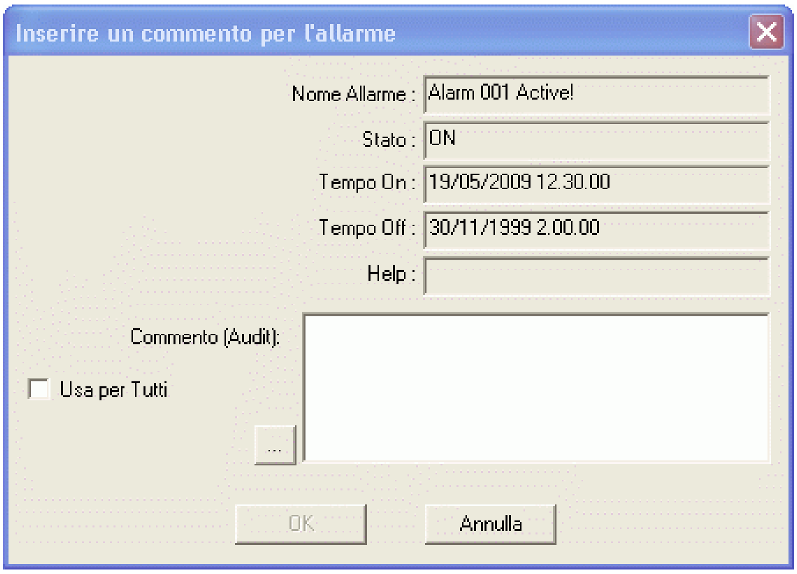
There may be times when the above described operations need not only the operator user's authentication but also validation from the Process Manager before a Tag change can be made effective. However, authentication must only be requested from Process Managers with the same level or higher.

As each process has different needs from the next, Movicon does not manage this function automatically the user must provide a Template being a graphic object that can be called up every time an edit request is made. This object allows access, user identification and data settings (Tag variables), which can be linked to both Tracing function and a Data Logger which have been configured to record the values relating to each status change.

Alarm Acknowledgment Comment (Audit Trail)

In many cases before the user acknowledges an alarm, it may be required to enter a comment (Audit). When a comment is entered it will be recorded in the historical log together with the alarm's ACK event.

The possibility to enter alarm acknowledgement comments can be enabled by checking the "Comment on ACK (Audit Trail)" option found in the alarm threshold properties window. When this option is activated and the alarm is acknowledged, a window will appear showing the information relating to the confirmed alarm and a space within which the user can enter his/her comments. The edited comments will then be recorded in the Historical Log's Alarm table's "CommCol" column.



Inserire un commento per l'allarme

Nome Allarme : Alarm 001 Active!

Stato : ON

Tempo On : 19/05/2009 12.30.00

Tempo Off : 30/11/1999 2.00.00

Help :

Commento (Audit):

☐ Usa per Tutti

Alarms can only be acknowledged after the user has existed from the comment window with the "OK" button or otherwise cancelled with the 'Cancel' button. The comment window is also managed in network client projects, or when the command is used in a multi alarm selection, or when using the basic script interface, or with commands from the command list.

In order to protect alarms from unauthorized users, set a password level in the Alarm Window so that the user will be required to log on before being able to acknowledge the alarm in question.

Electronic Records

Electronic Records contain all the process information (dates, values, events) recorded electronically on files that must guarantee data integrity and prevent any unlawful handling from unauthorized persons.

All the information recorded on file by Movicon is called “Electronic Records”.

In order to get the Movicon Electronic Records standard ready, the following indications and the guidelines contained in this document need to be followed to guarantee security in data integrity and prevention against any unauthourized access and data tampering.

Data Security

Guaranteed Electronic Record security is absolutely fundamental in obtaining valid applications. The data recorded by Movicoin (Data Loggers, Log, Tracing) are physically built by:

- **IMDB: criptable XML text files** with an algorithm in 128 bits. To use this format you need to check the **“Cript File”** option to guarantee inaccessibility to external manipulation of historically logged data.
- **ODBC: Relational Databases** by means of the integrated ODBC manager. The data, therefore, physically resides in data files and tables that can be recorded on hard disk locally or on mass files residing physically in diverse servers. Thanks to the use of “safe” relational databases such as SQL Server, Oracle or others, Movicon uses protected accounts for accessing files. It is the user’s responsibility to configure the system so that no one can access files, by removing access rights to file both in the database itself and in the operating system folders access rights (Movicon run as service). Data security must be guaranteed by means of using the following procedures:

1. Always use a data format based on relational databases that provide access protection, such as Microsoft SQL or Oracle.
2. To avoid unauthorized access to files, User Account protection will need to be setup by using the access criteria explicitly for system administrators or program designers only (eg. With the same project protection password). This will impede access to data tables where authorization has not been provided.
3. Use the operating system’s access lock (Locked by Movicon) or access rights to operating system by using Movicon as Service. By doing this, file access through the operating system will be physically denied.
4. Do not share folders or disks when the station is operating in net, except for system administrator access.

5. Remove all rights to modify database records (Updates). Movicon lets new records to be inserted whose data cannot be accessed for altering no matter what the reason is.

The 21 CFR Part 11. regulations

Tips and suggestions on how to get your Movicon 11 project compliant with the 21 CFR Part 11 regulations.

PART 11—ELECTRONIC RECORDS;

ELECTRONIC SIGNATURES

Subpart A—General Provisions

Sec.

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 Impiego della firma.

11.70 Collegamenti tra firma e record.

Subpart C— Electronic Signatures

11.100 General requirements.

11.200 Electronic signature components and controls.

11.300 Controls for identification codes/passwords.

Authority: Secs. 201–903 of the Federal

Food, Drug, and Cosmetic Act (21 U.S.C.

321–393); sec. 351 of the Public Health

Service Act (42 U.S.C. 262).

Section	Specification
Subpart A	**General Provisions**
§ 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 § 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.
§ 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.
§ 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.

Section	Specification	Movicon Solution
Subpart B *§ 11.10*	**Electronic Records** **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:	**Movicon users are, alone, responsible in creating projects according to the regulations indicated by this act. The Movicon project must be configured for correct User Profile management use by exploiting the security criteria and unequivocalness of Movicon.** **Procedures must be taken against any kind of data mishandling by using IMDB with crypted historical data or ODBC with Movicon configured as Windows XP/Vista/7 Service, so that the operating system's security features can be used in their entirety when accessing recorded data.**
(a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	**Movicon users must validate their applications in appliance to the FDA act. Users can develop and/or execute the validation of programs and protocols themselves or delegate this job to someone else. Validation should be done according to the system's life cycle (SCL).**
(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	**The Movicon application must be capable of recording data in electronic format by using a safe format (crypted IMDB or safe databases such as SQL Server,**

	contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	**Oracle...).** **The records can be recorded by using the Data Logger, Historical Log and Tracing resources. All the historicals track down the Active User, date, time and reason why recording took place. The Movicon Historical Log automatically records the users and system events. The records are recorded in a database where data can be accessed safely and reviewed in the same project by using either the viewers, the Reports functions or by using the purposely created Basic Script procedures.**
(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	**Records stored by Data Loggers, Historical Logs or Tracers are archived in a crypted IMDB or ODBC with access security to protect them against undesired or unauthorised access. The security against mishandling data stored in the ODBC can be guaranteed by using the operating system's protection features and by running Movicon as a Windows XP/Vista/7 Service, or by using the protection offered by safe Relational DBs (SQL Server, Oracle, etc.) Archived records must be kept stored for an adequate period of time (at least one year). Movicon provides archives, which can be sized and automatically recycled as desired by the programmer with backup procedures implemented with the appropriate Movicon functions.**

(d)	Limiting system access to authorized individuals.	**The Movicon security functions and password management must be used for limiting access to operations carried out in the project. Movicon automatically manages access levels, encrypts passwords (project encryption), controls uniqueness and discourages any unauthorized access attempts by recording these events on Log. Furthermore, Movicon can be used as Service in the Windows XP/Vista/7 environment and shares passwords with the operating system's domain.** **Both Movicon and the operating system manage (when enabled) Auto-Logoff (timeout) so that the inactive user only remains enabled in the system for the limited period of time set before being automatically logged off.**
(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.	**All the records stored on Database by Movicon must include the date and time (in PC's local time or synchronized GMT origin) both for Data Loggers and for recorded events (ODBC Historical Log). User LogOn and LogOff events are also recorded.** **When more than one station is being used, Client/Server architecture, the server must be made ready to synchronize the clocks of clients in the system to get one communal date and time reference.**
(f)	Use of operational system checks to enforce permitted sequencing of	**The Movicon User is responsible for applying the necessary**

	steps and events, as appropriate.	**security procedures to permit the sequencing of steps and events. The automatic batch procedure can be used to manage operations and recipes in a step-by-step sequence.** **All the set or modified data can be recorded by using an appropriate function (Datalogger or Variable Tracing).** **Clients must develop systems which combine recipes, logic and security in order to verify whether all operations are being carried out correctly.**
(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 Movicon security functions and password management must be used to limit access to operations in the project. Movicon automatically manages access levels, encrypts passwords (project encryption), controls uniqueness and discourages any unauthorized access attempts by issuing a warning of this event. Furthermore, Movicon can be used as Service in the Windows XP/Vista/7 environment and shares passwords with the operating system’s domain.** **Both Movicon and the OS manage (when enabled) Auto-Logoff (timeout) so that the inactive user only remains logged on to the system for a set limited time period before being automatically logged off.**

(h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	**To guarantee data source validity, Movicon projects should be created with Client/Server configurations for each workstation exiting in the system with all recorded data filed safely in the Central PC (Server) redundant and protected against any kind of mishandling. (Windows XP/Vista/7 OS and the used database security).**
(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.	**Movicon clients are responsible for ensuring that all persons involved with system management are fully qualified with the right training and information and enough experience to carry out the tasks assigned to them.**
(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.	**Movicon clients are responsible for setting up policies and procedures to adapt the use of applications developed in conformity with the FDA regulations.**
(k)	Use of appropriate controls over systems documentation including:	**The Movicon users must establish the right procedures to use and control documentation relating to the developed application.** **The Movicon User's Manual can be**

(1)	Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	**referred to whenever necessary and is available in paper form or on Cd-Rom in .PDF electronic format and therefore cannot be changed in anyway by the client.** **Even though Movicon Clients are not directly responsible for the contents of this manual they must however ensure that it is distributed, accessed and used correctly.**
(2)	Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	**The Movicon user must set up the right procedures to ensure that any modifications done to the documentation relating to the developed application or platform are carried out correctly and kept under complete control. The Movicon User's Manual should be referred to and all modifications must always be referred to the right manual version of the software installed.**

<table>
<tr><td><b>§ 11.30</b></td><td colspan="2"><b>Controls for open systems.</b></td></tr>
<tr><td></td><td>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 § 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.</td><td><b>Movicon clients are responsible for setting up the right procedures and functions supplied by the systems being used (Movicon, Windows, SQL) to ensure that the system is kept in conformity with the FDA act.</b></td></tr>
</table>

§ 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;	**Movicon has been designed to include the unique user name (name of logged on operator) in all records stored.** **Username information must be inserted whenever requested when using Data Loggers. Movicon must be configured to record the name of the user logged on (username must be unique to that individual). Username uniqueness is managed by Movicon.**
(2)	The date and time when the signature was executed;	**The date and time are automatically recorded in the Movicon historical logs. It is advised to use GMT otherwise server and client times and dates must be synchronized and the chosen format must be coherent with that of the Data Loggers.**
(3)	The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	**All system events are automatically recorded in the Movicon Historical Log together with the user name and event type (eg. ACK, RESET, etc) using**

		ODBC drivers. However, it is possible to customize event recording by using the Data Logger.
(b)	The Items identified in paragraphs (a)(1), (1)(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).	**All records should be stored in a crypted IMDB database or a relational ODBC with the necessary security, and must be kept stored for an adequate period of time.** **Recorded data can be displayed in the project by using the right viewer tools or viewed in Report printouts using the purposely created Basic Script procedures.**

§ 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.	**Every record stored by the Data Loggers must include the unique name of the user (operator ID) logged on to the control system and responsible for the operations carried out at that moment.** **The Movicon security functions and password management with user profiles** **must be used for limiting access to operations in certain areas of the project.** **Movicon automatically manages user profiles with access levels, password encryption (project encryption) and controls user ID authenticity and uniqueness and discourages unauthourised access attempts by recording them on the Log.** **In addition to this, Movicon can be used as Service in the Windows XP/Vista/7 environment and shares passwords from the OS domain.** **Both Movicon and the OS manage (when enabled) Auto-Logoff (timeout) so that the inactive user only remains logged on to the system for a set limited time period before being automatically logged off.**

Section	Specification	Movicon Solution
Subpart C	Electronic Signatures	
§ 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. .	**Each electronic signature used in the system must be unique to that individual and not be reused or reassigned to any other person.** **The Movicon security management, like that of the Windows XP/Vista/7 OS, does not allow user duplication which means the same electronic signature cannot be reused or reassigned to another individual.** **The Movicon User Profiles (electronic signatures) are individual and unique to the user they were originally assigned to.**
(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.	**Movicon users who develop applications in conformity with the FDA act are responsible for carrying out the right security checks to control and verify the authenticity of each individual person before they are assigned an electronic signature to access system data.**

(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.	**Movicon clients using FDA ready applications are responsible for certifying that the electronic signatures in their system are the legal equivalent of traditional handwritten signatures whenever requested by the FDA agency.**
(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.	

§ 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.	**Both Movicon and Windows XP/Vista/7 employ a combination of User ID and Password (encrypted with the project) to identify users. User identify must be unique to that individual when recording data. The User Profile descriptions are unique to each single user they refer to in Movicon (Electronic signature).** **Movicon can be configured as Windows XP/Vista/7 Service in order to use the entire security features of the OS in accessing recorded data.**
(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.	**Before a continuous period of controlled system access is allowed to begin, the Movicon project will request a Log On procedure with at least two identification components (User ID and Password).** **The Active User's Electronic Signature is recorded when that user logs on.** **Any subsequent signings done during this period can be recorded with the User's ID only.** **The Movicon Automatic Log-Off, with a preset timeout, is used for limiting the continuous period of system access. The Movicon User should use this function for deactivating any users who are still inactive in the control system after a certain period of time.**
(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;	**The user must administer the right procedures to ensure that the identifications of users in non biometrics identification systems (eg. badge reader, transponder) are genuine.** **This procedure should include a control check to require the collaboration of two or more individuals to identify a user who attempts to access data by using another individual's electronic signature and not his/her own (this is to ensure that a badge, for instance, is not used inappropriately by third parties). It is the user's responsibility to use the functions provided by Movicon or Windows to impose expiry time periods on passwords as well as ensuring that only legitimate owners of passwords can access (by enabling the "Must Change Password" or "Expiring Password (Days)" to impede the system administrator from knowing both the User identification and password of individual users.**
(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.	
(b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	**Control Systems can be accessed by identifications based on biometrics. Biometric devices are available on the market and the Movicon users, developing applications compatible with the FDA regulations, or manufacturer of the installed biometric devices, are responsible in certifying that the electronic signatures based on biometrics are unique and individual to each user and cannot be used by any other person not being the genuine and originally**

		registered user. **Biometic systems can be managed directly in the Movicon project, by using the necessary Basic Script interfaces or managed by the OS that identifies users and shares its domain with the Movicon project users.**

§ 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:	**For a system to meet the requirements stipulated in these regulations it must be provided with access security in the form of user identifications with a combination of at least two components: User ID and Password.** **The user must own an "electronic signature (Profile description) that must be unique to that user in the system.** **Movicon also permits OS Domain sharing.**
(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.	**Movicon controls the uniqueness of each inserted user profile. Movicon must be configured as a service in the Windows XP/Vista/7 environment so that the OS security functions can be used in their entirety to ensure that passwords for accessing data have controlled longevity and complete uniqueness.**

(b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	**The user is responsible for setting down the criteria for carrying out periodical checks and revisions on passwords or the re-issuing of expired passwords. Movicon also permits passwords to have expiry dates.** **Movicon also permits OS Domain sharing.**
(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.	**Movicon Users must create projects with procedures that conform to the FDA regulations.**
(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.	**The Movicon password management discourages any unauthorized attempts to access system data (The response time is extended on each password entry attempt which is also by Windows). Any attempts made after the 5th failed attempt are recorded as acts of system violation.**
(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.	**Movicon Users are responsible for adopting the right procedures to ensure that system biometrics and access management work correctly and are not tampered with or mishandled in any way.**

This document has been developed by:

Progea Support Team

Modena, Italy

Dated: 20 February 2002

Revision: 6 March 2012 (for Movicon 11)

Specification FDA CFR 21 Part 11 by:

William B. Schultz,

Food And Drug Administration

Deputy Commissioner for Policy.

Dated: March 11, 1997.