Premium HMI and FDA 21 Part 11 regulations

Introduction

This document contains a brief explanation of the FDA CFR21 Part 11 regulations. It describes then the procedures and actions to take, in order to design a Premium HMI project which can be compliant with the FDA 21 Part 11 regulations.
This document has been written to inform developers about its concepts and the best way to apply it with digital data recording functions and in the “electronic signature” use as required by the FDA regulations.
This document has no legal value and ASEM S.p.A. does not take any direct responsibility of its contents. It is still the designer/customer’s responsibility to verify the application has been developed according with the above mentioned regulations along with any updates that may have been made.

Version	Description	Date
1	First emission	10/04/2012

Table of contents

1 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 to build automation and control systems in conformance with the CFR21 Part 11 regulations, it is required all recorded data is strictly related/linked 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, 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.

1.1 Electronic Records

All significant process data on production quality and regularity must be permanently recorded and not tampered. 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.

1.2 Electronic signature

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

2 Automation system requirements

The Control Systems must be capable of acquiring the status and behavior of the process's variables in real-time.
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.

2.1 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 not editable 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.

2.2 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" combination 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.

3 General concepts to support the regulations

The concepts described below define how to use Premium HMI to develop projects compatible with the act and its regulations discussed in this document.
A list of the main concepts has been put together 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 Premium HMI, is compliant with these requirements.

3.1 Security

- The Premium HMI project must be encrypted (Premium HMI uses a 128 bit encoding) so that all the configurations and passwords used in the project are accessible from the outside.

- Premium HMI 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). Premium HMI 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.

- 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 Win2000/XP 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 Premium HMI project must use the User Password Profile management correctly, which involves the entering of a Password, UserID, User Name and Access Level. Premium HMI 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 Premium HMI 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 Premium HMI operating stations are allocated in safe places and that they are accessible to authorized personnel only.

- The Premium HMI AutoLogOff function must be used in systems in continuous use.

- Premium HMI has tools and procedures that can be used for discouraging any unauthorized access attempts and are the same as those used in the Win2000/XP operating system as required by the regulations. After the third failed attempt to access, Premium HMI 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 fifth unauthorized Log On attempt) Premium HMI will display and record the event in the Historical Log in order to safeguard against and control any further system violations.

3.2 Digital Recording / Electronic Signature

Premium HMI 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 Premium HMI 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 Premium HMI 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 encrypted 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 Premium HMI 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 Win2000/NT/XP 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 2000/XP OS functions or with the Basic Script codes for third party products.

3.3 Validation and Documentation

Some of the requirements specified in the regulations are not altogether implemented in software applications.
These Part 11 requirements can be satisfied if the customer 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 Premium HMI 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 (Premium HMI, Windows).

3.4 Other

All the data must be stored in a relational database, which fully meets the necessary security requirements (ie. IMDB encrypted data, SQL Server or Oracle with the relevant protection) and protected from any violation to or tampering of the security functions belonging to the Win2000/XP 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).

4 Configuring the project

To get a Premium HMI 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 are suggested below.

4.1 Security

The project must be configured in its General Properties by selecting “Crypted Project” and “Crypted 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.

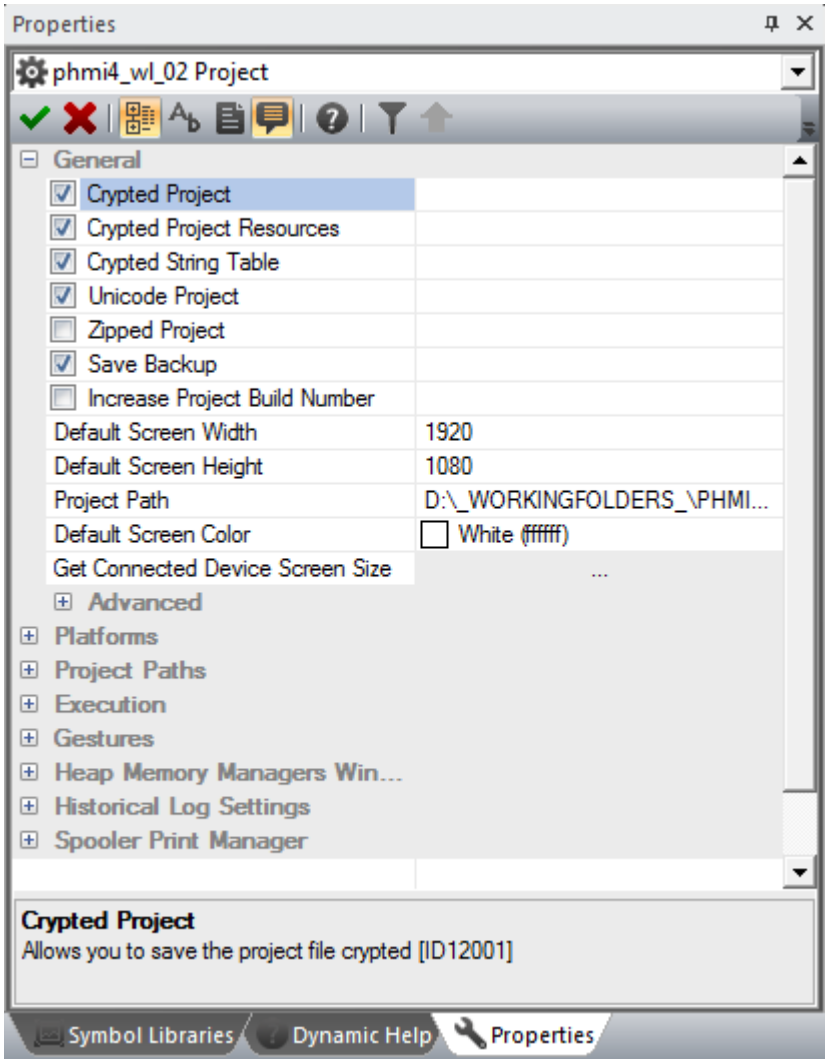

Figura 1

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

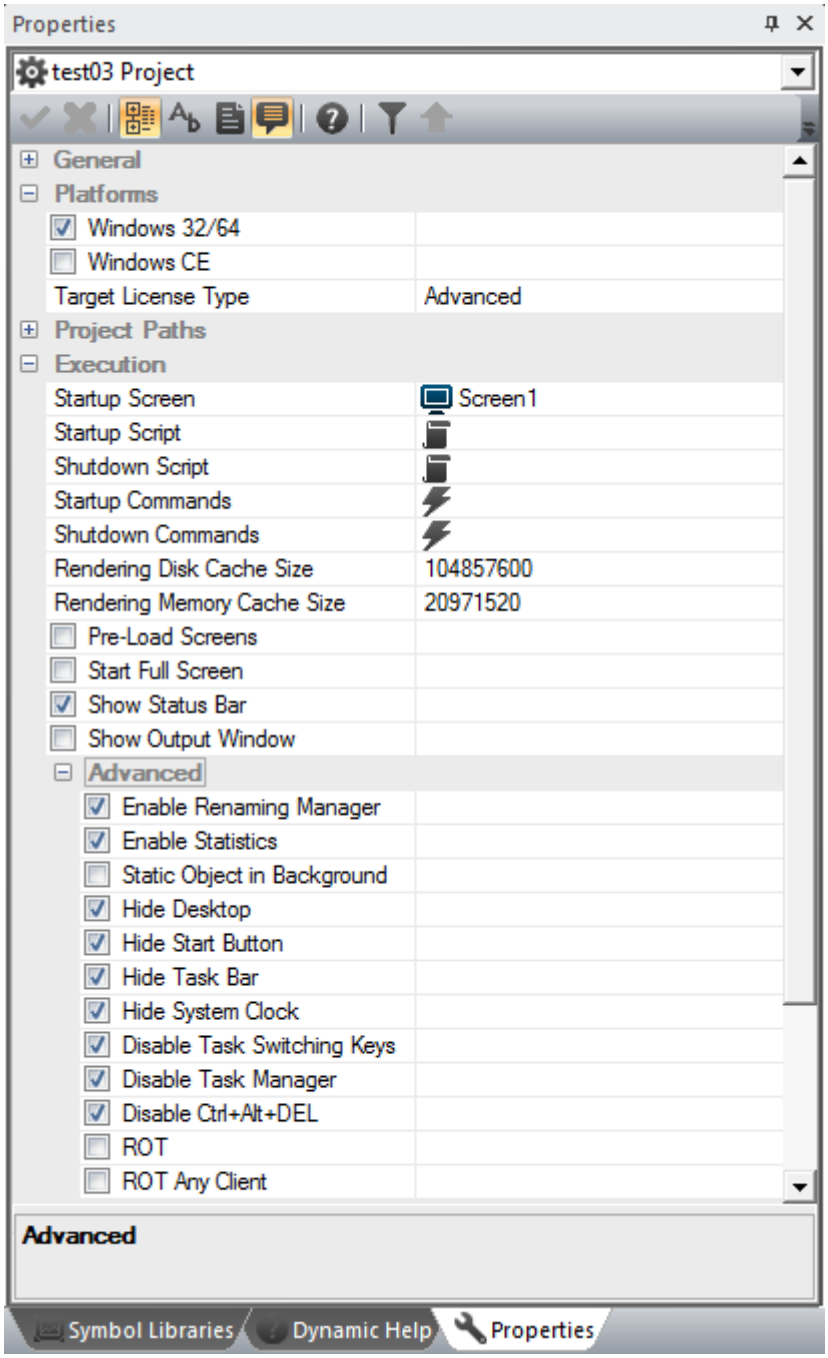

Figure 1

4.2 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.

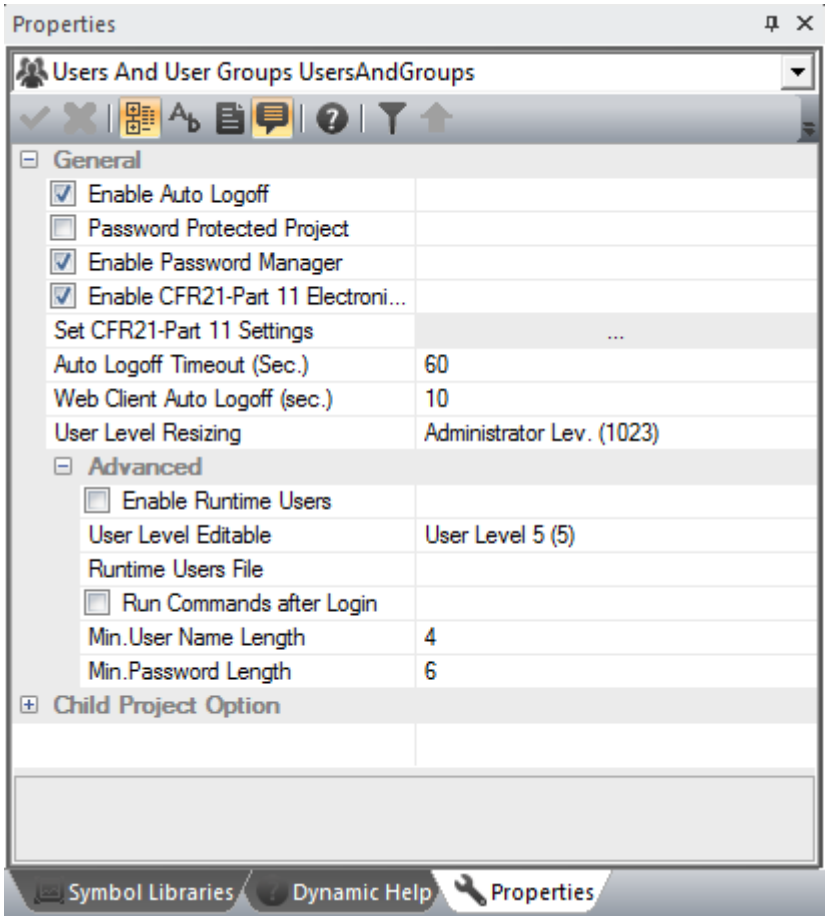

Figure 2

4.3 User Passwords

Each user or group, who has access to commands or process interaction, must be properly handled inserting security options in the project.

Users are configured 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.

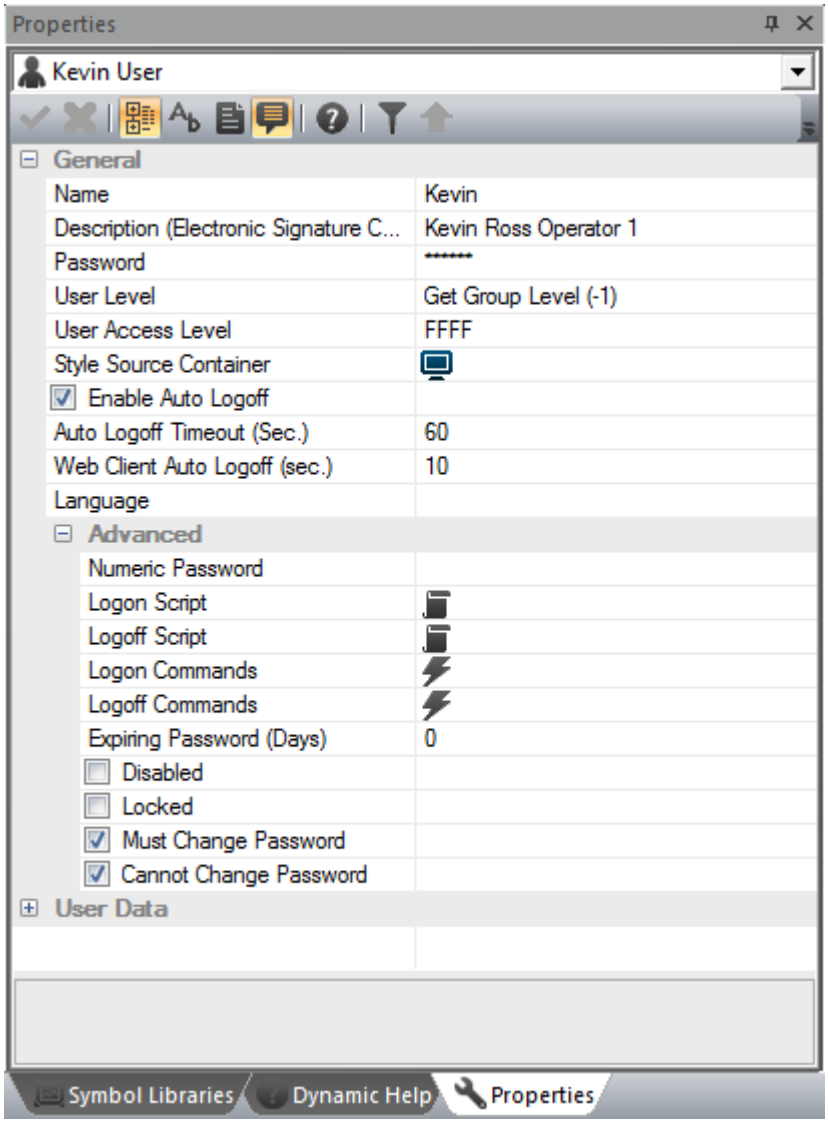

Figure 3

4.4 Command access/execution

- 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 Premium HMI 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.

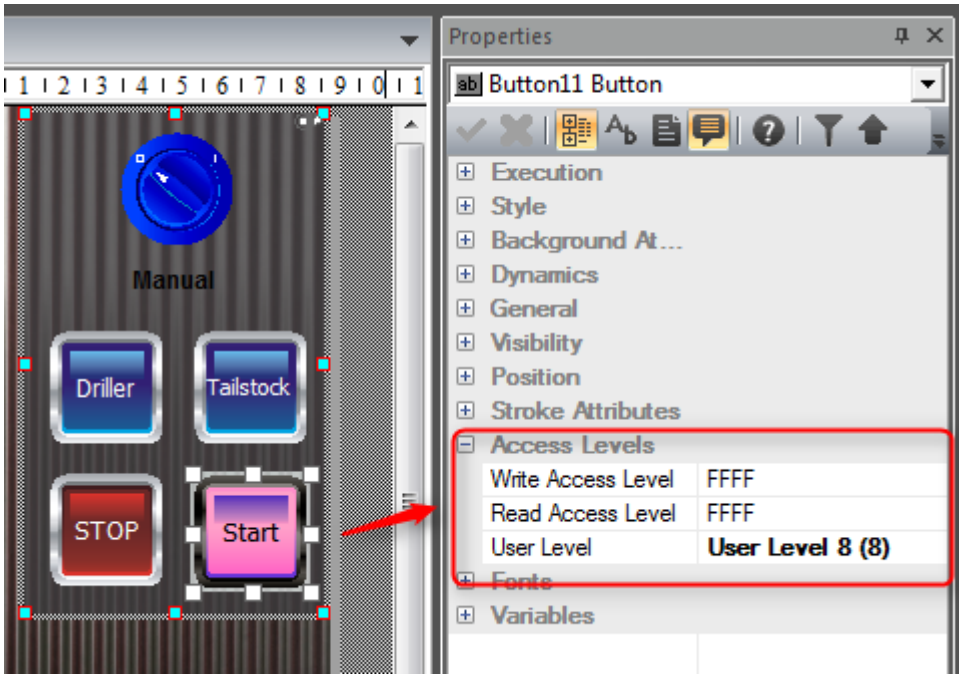

Figure 4

4.5 Operating System Access

Premium HMI provides the possibility to block and deny operating system access.

Lockout Windows access from Premium HMI: to prevent unauthorized access in the system you need to select the entire project's Execution Properties which deny access to the Operating System and Desktop. When Premium HMI is started up these will deny access to Windows according to the settings, which have been activated (described above).

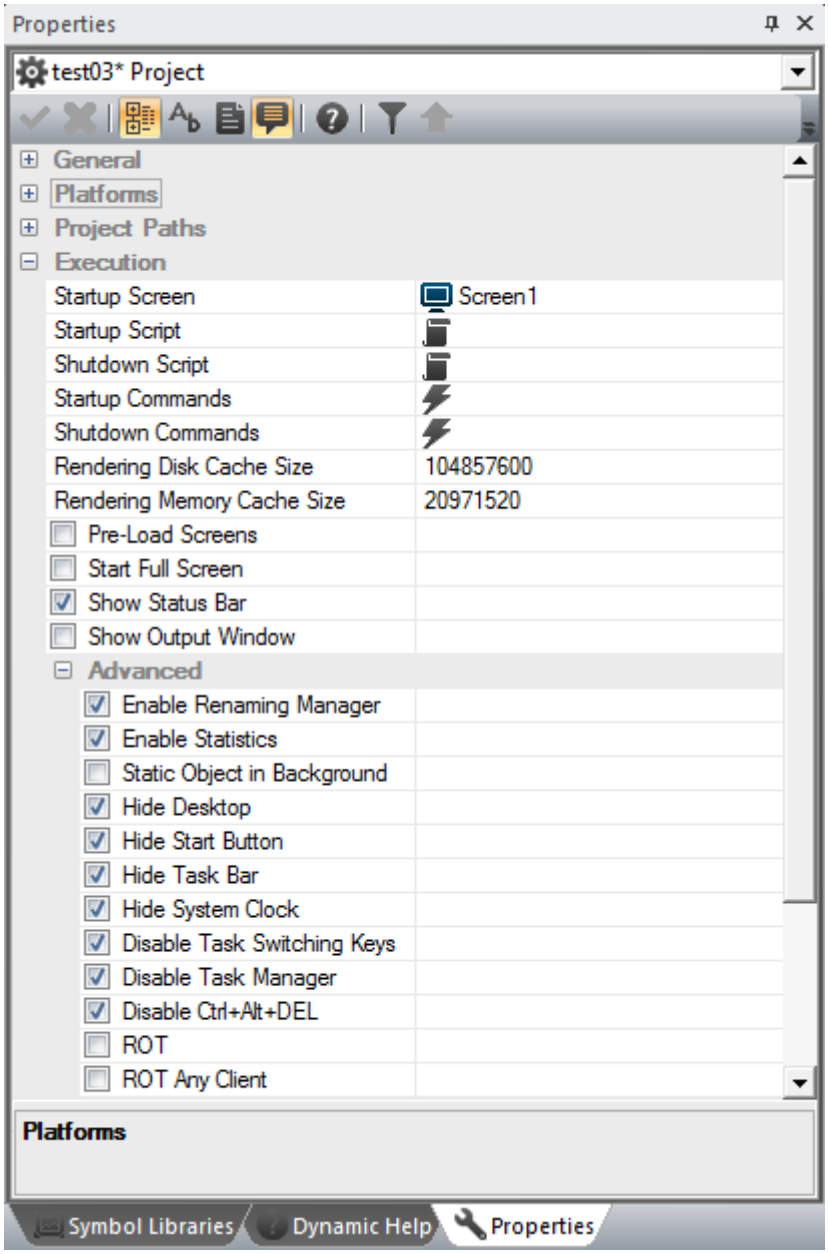

Figure 5

4.6 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.

Some examples:

It has been tested 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 Premium HMI project users can be associated by using the appropriate VBA script module. This biometric system can be completely integrated into the project using the Premium HMI “User Password –Fingerprint” association.

Premium HMI 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 recognized 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 (WinXP 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 Premium HMI application by using the appropriate Basic Script interface.

4.7 Recording data (Audit Trail or Tracing)

Premium HMI provides the possibility to trace all the status changes of each variable which has significant relevance 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).

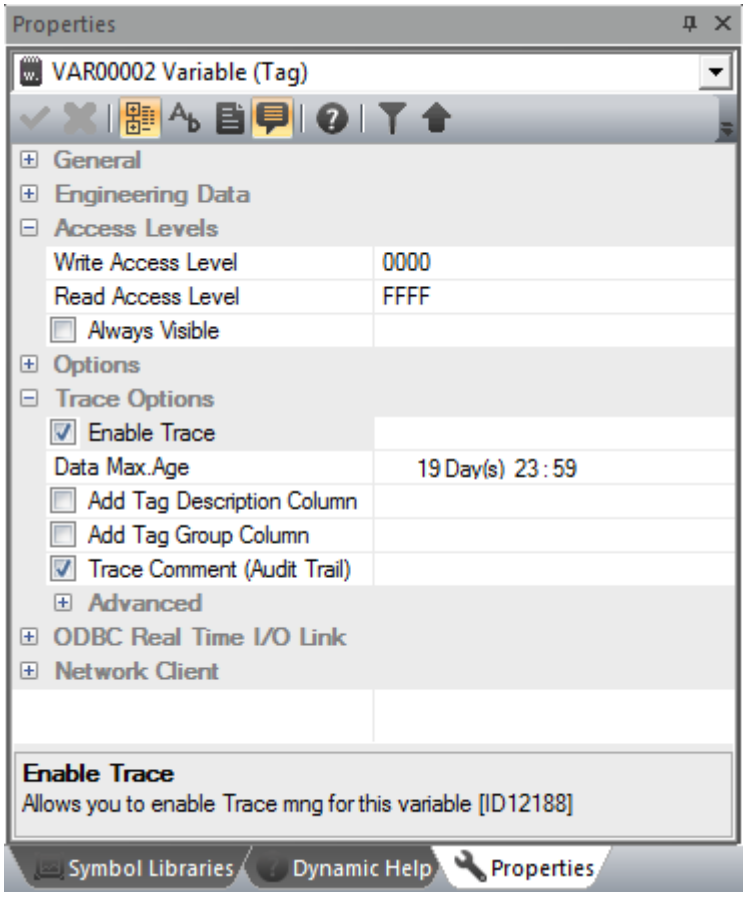

Figure 6

4.7.1 Audit Trail

In many cases, before the user can proceed in making any process variable changes (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 marked in the Trace Property beforehand.

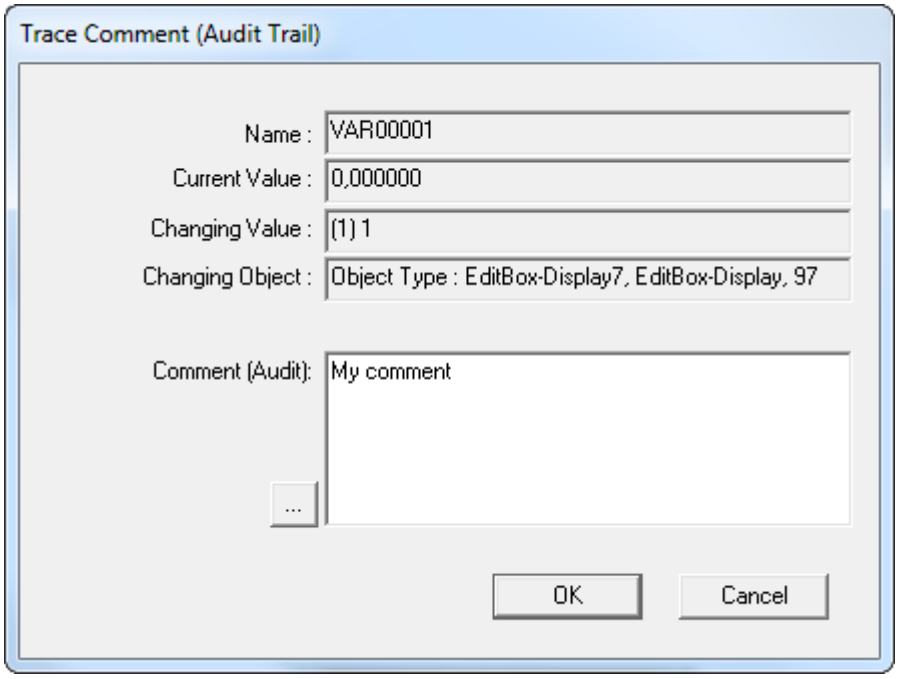

Figure 7

Premium HMI 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 is frozen. Any other process, such as the drivers, the IL logic, basic scripts, cannot change it.

4.7.2 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, Premium HMI 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.

4.8 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 Premium HMI is called "Electronic Records". In order to get the Premium HMI 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 unauthorized access and data tampering.

4.8.1 Data Security

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

IMDB: Encryptable 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, Premium HMI 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. 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 Premium HMI) or access rights to operating system by using Premium HMI 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). Premium HMI lets new records to be inserted whose data cannot be accessed for altering no matter what the reason is.