Realised by:
HEMATIS

White paper Schneider Electric/Hématis

SCHNEIDER ELECTRIC's products compliance with 21 CFR part 11

FDA 21 CFR § 11 Electronic Signature/Electronic Records: Implementation of the rule to HMI Magelis™ family integrated with following products:

- Vijeo Designer™
- IDS

SYNOPSIS

The purpose of this report is to evaluate Schneider Electric products Vijeo Designer™, associated with IDS software, suitability to be integrated in automated industrial solutions fully compliant with 21 CFR part 11 regulation. It is reminded that equipments investigated in following report are Programmable software associated to the use of the set of HMI Magelis™ of Schneider Electric.

Producing and maintaining records are not their first intent. However Schneider electric did realise significant effort to allow easy development of compliant with 21CFR part 11 automated solutions using tools provided by Magelis™ HMI family and associated development package software Vijeo Designer™ including IDS . IDS has been specifically developed to ease 21 CFR part 11 compliance for Vijeo Designer™.

Schneider Electric supplies complete set of secured tools to provide industry with automated solutions easily protected considering any element compliance possibilities and requirements.

This report does furthermore remind policies, procedures and best practices required for compliance and recommendations for users and systems integrators. These may be used as guidelines to implement solutions for regulated industries using Magelis™ HMI with applications developed with Vijeo Designer™ IDS package.

Edited by Schneider Electric
Industries SAS
35 rue Joseph Monier
Rueil-Malmaison
March 2010

Summary

It is reminded that no supplier can claim turnkey Part 11 compliant system. Part 11 compliant system requires not only proper technical implementation, and validation, but suitable user procedural and administrative controls.

- System architecture and its integrity
- Specific software application

May or may not provide robust and easy basis for user organisation compliance to Part 11 depending on both factors :

- Intrinsic hardware and Software capability
- Software application functional development

Software specific solution resulting from User requirement specification and functional analysis are essential for compliance. However hardware and systems architecture may or may not provide easy tooling to implement convenient complying solution.

This report concludes that using application developed with the Package Vijeo Designer and IDS for Magelis™ HMI will provide a good basis for a flexible and easy to implement 21CFRpart 11 compliant system. IDS has been specifically developed to allow for easy process datas retrieval and organisation and to comply with 21CFR part 11. Magelis™ HMI and associated development package software Vijeo Designer™ IDS have attributes which allow them to be preferred tools to develop industrial solutions fully compliant with 21CFR part 11 for regulated industries.

Tools which are required are :

- Vijeo Designer 5.1 and following version
- IDS
- Application Program interface
- Associated Operating Systems

Report proposes solutions combining those tools to allow easy implementation of compliant industrial solution.

Proposed solutions are not the only one and integrators may eventually use other external software to realise compliant systems.

Schneider Electric sales services are available to support and assist development of complying solutions. Contact your local vendor.

I. Introduction : SCOPE OF 21 CFR PART 11

SCOPE

Food and Drug Administration recognizes that the implementation of paperless systems can provide a wide variety of benefits including, among other things, increased speed of information exchange, improved ability to integrate, trend, search and retrieve batch and other production related data. These improvements can lead to a reduction in both errors and costs related to data storage and, ultimately, to improve quality and efficacy of product.

However Agency is concerned that possible deviations linked with uncontrolled systems operation and data documentation not controlled and lacking of transparency, for which it may be difficult to evaluate accuracy and performance. Consequently to encourage beneficial developments of technologies and guaranty the same level of controls and quality for consumers FDA does enforce regulation, 21CFR Part 11.

Part 11 establishes the criteria under which electronic records and electronic signatures are considered as equivalent to paper records and handwritten signatures executed on paper.

HISTORY

During the 1990's, the pharmaceutical industry sought guidance from the U.S. Food and Drug Administration (FDA) in the development of a uniform approach to the acceptance of paperless systems. As a result, the FDA issued its Final Rule on electronic records and electronic signatures ("21 CFR § 11," "Part 11," or "the rule") on Mar. 20, 1997; the rule took effect on Aug. 20, 1997.

Part 11 establishes the criteria under which electronic records and electronic signatures are considered as equivalent to paper records and handwritten signatures executed on paper. The rule applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in FDA regulations. In addition, documents submitted to the FDA but not necessarily required by the agency also fall under the requirements of the rule. Currently the FDA will accept electronic submissions of documents (in whole or part) that are identified in Public Docket 92S-0251 as being the type of submission the agency accepts in electronic form. Those forms include Biologics License Applications (BLA), Product License Applications (PLA), Establishment License Applications (ELA), New Drug Applications (NDA), Biologics Market, and Basic Information re Submission of Notices of Claimed Investigational Exemption to Center for Veterinary Medicine (CVM). Part 11 does not apply to paper records transmitted by electronic means. Understanding the applicability of the underlying FDA regulations, or predicate rules, to the records being generated is critical to developing Part 11 compliance solutions.

Since regulation have been enforced agency did precise its views and current interpretation through following industry guidance

- Computer System Validation Guide
- Glossary Guide
- Time stamps Guide
- Maintenance of electronic records Guide
- Copies of electronic records Guide

However interpretations of the rule have been very extensive and drove industry to require agency to precise its views dealing with scope and application. Consequently agency decided to review its policy guides. In February 2003 agency did propose a "draft guidance" to industry which was entitled "scope and application" for comments.

Reviewing period did finish April 28th 2003. From that date FDA did precise it has decided to review the rule itself. Agency intend is to clarify its view mainly for scope and application. This would be based on risk analysis assessment. Analysis would eventually be performed by systems users to determine wherever part 11 will fully apply.

Consequently Schneider electric approach will not be fundamentally questioned in its principle. Evolvement of part 11 may eventually lead Schneider Electric to reshape its schedule of comments and recommendation to fit with latest regulations summary.

SCOPE AND APPLICATION

Part 11 establishes the criteria under which electronic records and electronic signatures are considered as equivalent to paper records and handwritten signatures executed on paper. The rule applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in FDA regulations. In addition, documents submitted to the FDA but not necessarily required by the agency also fall under the requirements of the rule. Currently the FDA will accept electronic submissions of documents (in whole or part) that are identified in Public Docket 92S-0251 as being the type of submission the agency accepts in electronic form. However production equipments are not directly to be considered in License applications processes.

Understanding the applicability of the underlying FDA regulations, or predicate rules, to the records being generated is critical to developing Part 11 compliance solutions.

DEFINITIONS IN PART 11 OF 21CFR

- Biometrics (21 CFR § 11.3(b)(3)): 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.

- Closed System (21 CFR § 11.3(b)(4)): An environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

- Digital Signature (21 CFR § 11.3(b)(5)): 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.

- Electronic Record (21 CFR § 11.3(b)(6)): Any combination of text, graphics, data, audio, pictorial, or other information represented in digital form that is created modified, maintained, archived, retrieved, or distributed by a computer system.

- Electronic Signature (21 CFR § 11.3(b)(7)): 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.

- Handwritten Signature (21 CFR § 11.3(b)(8)): 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.

- Open System (21 CFR § 11.3(b)(9)): 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.

REQUIREMENTS OF 21 CFR § 11

In order for organizations to comply with Part 11, a number of requirements must be met. These requirements generally concern the authenticity, integrity and confidentiality of the electronic records and signatures. Any computer system utilizing electronic records and signatures must be validated according to generally accepted industry standards associated with a software development life cycle, to ensure its accuracy, reliability, consistent intended performance, and ability to discern invalid or altered records. Validation is defined by the FDA as "the process of establishing documented evidence which provides a high degree of assurance that a system will consistently perform in accordance with its predefined specifications and quality attributes" (Ref: FDA, Glossary of Computerized System and Software Development Terminology). The system must be able to generate copies in both human readable (i.e., in plain text) and electronic form that are accurate and complete.

Several types of checks must be built into Part 11 compliant systems including:

- System checks that enforce the sequencing of events, where required
- Authority checks that determine who has access to the system and at what level
- Device checks that determine the validity of sources of data being entered into a system

Systems that comply with Part 11 must be able to generate an audit trail. An audit trail is a record showing who has accessed a computer system and what operations he or she has performed during a given period. Any such audit trail must be secure, computer-generated and time-stamped; cannot obscure previously changed data; must identify the person responsible for making the change; must include both the original and changed data; and must be available for review and copying by the FDA. Audit trail documentation thus generated is required to be retained for a period at least as long as that required for the subject electronic records, either pursuant to a predicate rule or to the organization's own records retention policy.

Organizations using electronic records must also limit system access to authorized individuals. This requires a policy decision regarding the levels of access, the roster of individuals within each level, the criteria for determining eligibility to that level, and other system safeguards to prevent access to records by unauthorized individuals.

As with most FDA regulations, including most predicate rules, Part 11 requires that individuals who develop, maintain, or use electronic record and electronic signature systems, have the education, training, and experience to perform their assigned tasks.

CONTROLS FOR CLOSED AND OPEN SYSTEMS

Electronic record systems are subject to a number of procedures and controls under Part 11 depending on whether they are open or closed. The primary requirement applying to both closed and open systems is that they be validated to ensure their accuracy, reliability, consistent intended performance, and ability to discern invalid or altered records. The rule also requires that closed systems be able to generate accurate and complete copies of electronic records in human readable (i.e., in plain text) and electronic form such that the agency may inspect, review and copy those records deemed necessary. Electronic records must also be protected to enable accurate and ready retrieval for the duration of any required records retention period as discussed in the description of the audit trail above.

The rule also requires that certain checks be placed on closed systems, including:

- System checks that enforce the sequencing of events, where required
- Authority checks that determine who has access to the system and at what level
- Device checks that determine the validity of sources of data being entered into a system

The issue of record and signature falsification is a significant concern to the FDA; hence the rule requires that organizations using closed electronic record and signature systems must establish and follow written policies that hold their employees accountable and responsible for actions initiated under their electronic signatures. Organizations must also place appropriate controls over systems documentation regarding the distribution of, access to, and use of documentation for system operation and maintenance. Revision and change control procedures must be put in place to maintain an audit trail that documents time-sequenced development and modification of the electronic records system's documentation. Other procedures and policies are required for the protection of records, record retention periods, limits on system access, education and training, and revision and change control.

Part 11 requires the same controls over open systems as over closed systems; but, further, open systems must also be supported by procedures and controls designed to ensure the authenticity, integrity and confidentiality of electronic records created, modified, maintained, or transmitted over those systems. For example, such procedures and controls may include document encryption techniques and digital signature standards.

ELECTRONIC SIGNATURES – REQUIREMENTS

Part 11 sets forth general requirements for organizations that intend to use electronic signatures. Each electronic signature used within an organization must be unique to an individual and not reused or assigned to another individual. The identity of the individual must be verified by the organization (e.g., via birth certificate, drivers' license, passport) before assigning the individual an electronic signature. The organization must also certify in writing to the FDA that they intend to use their electronic signature as the legally binding equivalent of their handwritten signature; that certification must be submitted to the FDA in paper form. If required by the FDA, the organization may have to submit additional certification of its intention of use.

Biometric and non-biometric electronic signatures must exhibit certain characteristics reflective of their nature. Non-biometric electronic signatures must be composed of at least two distinct identification components (e.g., user ID and password); must be used only by their genuine owners; and must be administered and executed such that two or more individuals are necessary to duplicate the signature. Non-biometric electronic signatures also have specific requirements for use during periods of controlled access. If an individual executes a series of signings during a single period of controlled access, they must use all electronic signature components for the first signing and at least one secret component for each subsequent signing. If, however, signings are not performed during a single period of controlled access, each signing must use all electronic signature components.

Biometric electronic signatures must be designed to ensure that they cannot be used by anyone other than their genuine owners.

SIGNATURE MANIFESTATIONS AND LINKING

Part 11 requires that signed electronic records bear a signature manifestation, that is, a clear indication of the printed name of the signer; the date and time of the signing; and the meaning of the signing. Those records must be subject to the same controls as electronic records, and be available for review and copying by the agency. Electronic signatures, as well as handwritten signatures executed to electronic records, must 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

II. What is Schneider Electric Doing?

Schneider Electric/Square D has a long and substantial history in industrial automation, starting with the fact that one of their businesses (Bedford Associates, later called Modicon) was the original designers and manufacturers of industrial programmable logic controllers (PLC).

In June 2001, Schneider Electric contracted with Stelex-TVG to perform an evaluation of several products including CONCEPT™ (v2.5) PLC programming and operating software package, Modicon QUANTUM™ (140-CPU434xx, 140-CPU534xx) PLC family, MOMENTUM™ PLC family, and ONESTEP™ Generator (v1.3) process design tool for compliance with the rule. Stelex-TVG performed the evaluation by assessing the applicability of Part 11 to the applications. Key assumptions made during the evaluation were (1) the applications need to comply with all requirements of Part 11; and (2) the applications may potentially be used in open systems as defined in Part 11. A checklist based on the requirements of Part 11 was used, and each application was assessed for the applicability and level of compliance with the rule.

In April 2003, SCHNEIDER ELECTRIC contracted HEMATIS to perform complementary evaluation of several products including Modicon PREMIUM™, MICRO™, PL7, PL7dif, and Vijeo Look. This evaluation takes place in the frame of 21CFR part 11 reviewing process.
Following evaluation, SCHNEIDER ELECTRIC and HEMATIS propose a set of recommendation for users and systems integrators to implement operating systems fully compliant with 21CFR part 11.

SCHNEIDER ELECTRIC did further propose evaluation and 21CFR part 11 cook book for following integrated solutions :

- Vijeolook / Modicon PREMIUM™, MICRO™, /PL7
- Monitor/ Modicon PREMIUM™, MICRO™, /PL7
- Unity Pro

SCHNEIDER ELECTRIC did start development of corresponding identified solutions during summer 2004 for Modicon Premium™, Quantum using Unity Pro.

Unity Dif was specifically developed to ease traceability in accordance with 21CFRpart 11, and was introduced to market in May 2007.

In March 2010 Schneider electric is introducing Vijeo Designer™ new generation of software for its Magelis™ HMI family. Schneider Electric, in partnership with Productys is introducing IDS software specifically designed and implemented to allow easy retrievement, storage and customisation of production data. The package Vijeo Designer™, IDS has been specifically developed to allow for easy and smooth 21CFR part 11 compliance solutions.

III. Best Practices and Software Solutions

When it comes to consider what is really critical towards regulation for a computerised system used in the frame of a regulated manufacturing process many questions arise.
Firstly it is important to remind that what matters really is what is happening during processing. Therefore regulated industries using computerised systems controlling processes that may impact quality of products should focus on making sure that:

- Once the software application have been developed and validated (latest when the installation goes under change control) it is not possible to modify it without insuring full traceability of modification and identity of operators who have implemented the modifications
- That any software data that may be changed on purpose during production course is recorded and identity of those who did operate the modification is recorded

Secondly, organisation using electronic data to support compliance with predicate rules must ensure quality, integrity and security of critical data collected and stored during the production, once they have hit their final storage location.

MAGELIS™ VIJEO DESIGNER™ IDS

Customers are advised to implement the following practices and software solutions to meet the intent of Part 11 regulations for programming and operating software packages **VIJEO DESIGNER™ IDS™** for **MAGELIS™** . A detailed Part 11 checklist that served as a basis for these recommendations is included in this document.

In the following section, PANEL will be understood as any interface such as MAGELIS™ panels, Magelis iPC or standard PC.

1. Security

   - To limit system access, customers are advised to configure the **VIJEO DESIGNER™** Security Editor. **VIJEO DESIGNER™** administrators should create users and assign appropriate rights. Users must be required to create passwords and periodically change them through customers Standard Operating Procedure.

   - Customers are advised to further secure final datas storage stations by ensuring that they are configured to use Windows (version) domain security. Domain administrators should implement account policies on password aging, minimum password length, password uniqueness, and account lockout after a reasonable number of unsuccessful login attempts.

   - In the event workstations or Panels are used in a non-network environment, it is recommended that Windows (version) operating system be used on these systems. The local administrator should implement unique user accounts with policies on password aging, minimum password length, password uniqueness, and account lockout after a reasonable number of unsuccessful login attempts.

   - To prevent unauthorized use of passwords, Panel access will be disabled after an appropriate number of unsuccessful login attempts. The security engine will log any such events to the event logs, which should be periodically monitored by administrators.

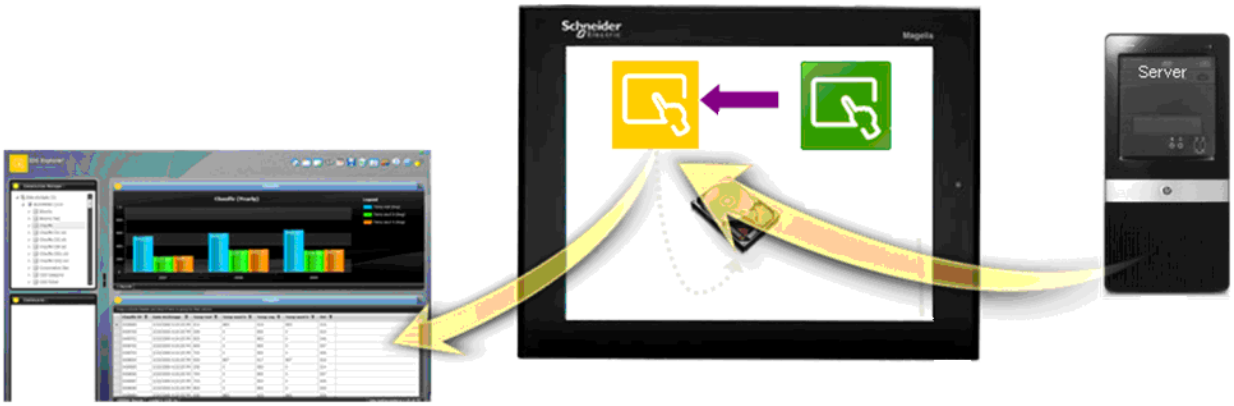
   - To limit the duration of a continuous period of controlled system access, a password protected screen saver should be configured to activate after a reasonable inactivity period. Some factors in determining the appropriate length of the inactivity period include physical access to the workstation and the number of potential workstation users.

   - To ensure the validity of the source of data input, customers must ensure that all workstations are placed in secure locations and that access to the workstations is limited to authorized personnel.

Furthermore **VIJEO DESIGNER™** provides continuously the information of the validity of the datas gathered by the workstation

- Also it is advised to use the **VIJEO DESIGNER™ functionality** to specify IP addresses authorized to access application program

- It is advise to implement customers Standard Operating Procedures to prevent uncontrolled software installation



2. Electronic Records/Electronic Signatures

- To comply with requirements on Electronic Records and Signatures the **VIJEO DESIGNER™** Online functionality should only be used for development purposes. **VIJEO DESIGNER™** software should not be used to control, override, or in any way manipulate the operation of HMI during any manufacturing operations. It is possible with **VIJEO DESIGNER™** to disable online access functionality. Furthermore **VIJEO DESIGNER™** allows for defining strictly authorized IP address to access applications programs. If customer choose this possibility they are reminded that security access of the pre-defined authorized IP workstations are to be protected and controlled in accordance with 21CFR part 11.

- Customers Operating Procedure will forbid during normal operation (ie run time) **VIJEO DESIGNER™** access to levels allowing program modifications
- Use of **VIJEO DESIGNER™** audit trail implemented with IDS. Audit trail will permit to identify any **VIJEO DESIGNER™** session start-up during production phase, locally or on IDS Viewer
- Use of IDS allows for comparison of applications independently of PC's and reports integrity checking
- IDS allows for controlling application signature during production. Therefore it is possible to check conformity of application used at any time manually or automatically.

- To ensure protection of records throughout the records retention period, customers are advised to archive datas gathered by **VIJEO DESIGNER™** using IDS. Customers also are advised to:
  a. Activate **VIJEO DESIGNER™** security editor

  b. Protect writing wherever critical sections of applications are identified

  c. Secure automatic application version retrieval and storage through "audit trail" implemented. Specify and develop a data retrieval and storage application using IDS

  When implementing these procedures, great care must be taken to document the overall procedures and the individual practices.

- Also it is advised to control and restrict IP addresses authorized to access **VIJEO DESIGNER™** program.

- It is furthermore reminded that the Final datas storage station shall be itself protected. Protection/Access rules shall be specified and will be developed separately

.

Validation and documentation

- Many of the requirements of the rule must be met by practices that are not software-based. In order to meet the validation requirement of Part 11, Customers must validate the application software in order to ensure accuracy, reliability, consistent and intended performance, and the ability to discern invalid or altered records. Customers may develop and/or execute the validation plans and protocols themselves or outsource these practices. The validation should follow an established system life cycle (SLC) methodology. GAMP recommendations are a good tool for project development and validation of automated production systems

- It is reminded that all support applications such as audit trails implementation automatic application versions storage procedures should be validated according to same principles
  In order to support users validation processes, Schneider Electric does provide: Qualification of hardware
  - Hardware qualification
  - **VIJEO DESIGNER™ and IDS** software validation
  - Training certificates for operators in charge of development and maintenance of systems
- To enable accurate and ready retrieval of **VIJEO DESIGNER™ and IDS** projects throughout the records retention period, customers are advised to create procedures outlining record retention periods and retrieval policies.

- In order to meet the authority checks requirement of the rule, customers must employ policies and procedures to verify the identity of the individual to whom an electronic signature will be issued.

- Customers must establish and adhere to written policies that hold individuals accountable and

responsible for actions initiated under their electronic signatures in order to deter record and signature falsification and to meet that requirement of the rule.

- Although customers are not responsible for control over the content of system operation and maintenance manuals, they should be responsible for establishing and maintaining controls over the distribution of, access to, and use of that documentation as required by Part 11.

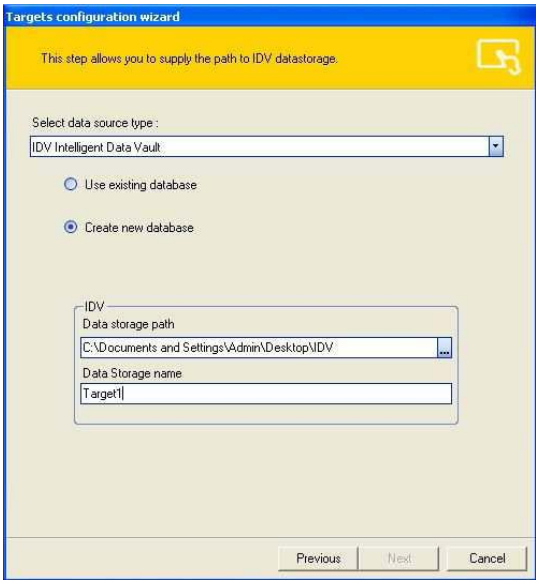
- Customers must verify the identity of the individual before assigning an electronic signature to him/her. Customers are also responsible for certifying in writing (in paper form) to FDA that they intend to use their electronic signature as the legally binding equivalent of their handwritten signature and, if necessary, submit additional certification of that intention to the agency.

- Customers should implement policies and procedures requiring users to log out of the application during periods of non-use.

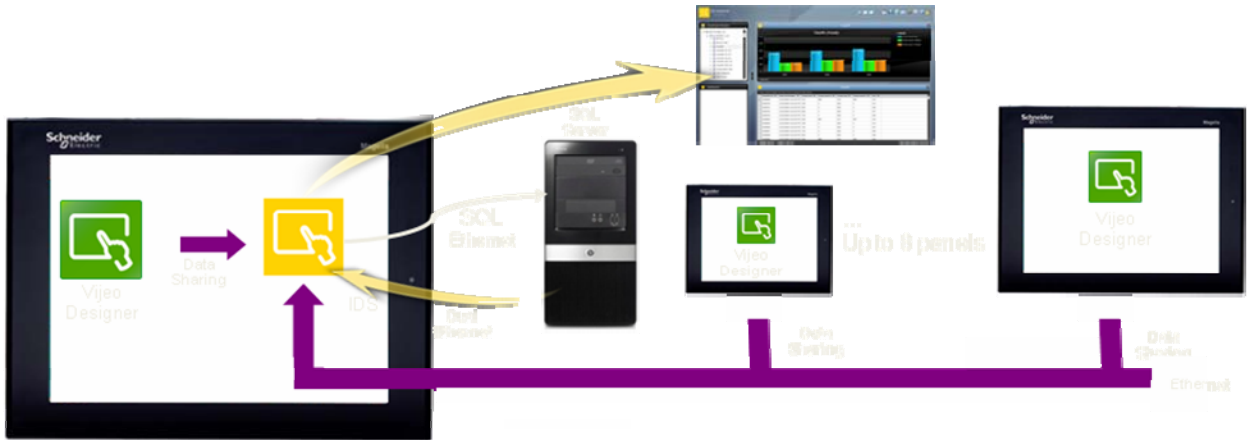
- Customers must create procedures for ensuring that identification code and password issuances are periodically checked, recalled, or revised.

V. CFR 21 § 11 Checking list for Schneider Electric products

Section n°	**Rule**	MAGELIS™ / Vijeo Designer™ / IDS
11.10	**Controls for closed systems**	
	Persons who use closed systems to create modify maintain or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:	Persons named by the rule are industrial using computerized systems. Architecture of procedures and their implementation is under their responsibility and shall be incorporated in their overall quality assurance systems.
11.10 (a)	Validation of systems to ensure accuracy, reliability, consistent intended performance,… …and the ability to discern invalid or altered records ***GAMP Interpretation:*** *In practice this means having an adequate audit trail, that can be searched for information. For example, to determine whether any changes have been made without the appropriate authorizations*.	Validation of systems and applications is undertaken during systems development phases. It covers both hardware conformity and application software validation. Schneider Electric does provide MAGELIS™ HMI qualified in the frame of Schneider Internal Quality Assurance policies. Development software Vijeo Designer™ associated are validated in the frame of Schneider Electric Internal QA policies. Associated IDS™ software to design and implement data retrieval transfer treatment and storage is validated through in the frame of Productys Internal QA policies. Those tools provide highest guaranty to develop consistent architectures with accurate coherent and validated application software. Specific customized interfaces developed to ensure application protection and system audit trail will be case by case validated. See below for audit trail implementation recommendation

Section n°	Rule	MAGELIS™ / Vijeo Designer™ / IDS
11.10	**Controls for closed systems**	
11.10 (b)	The ability to **generate accurate and complete copies of records** in both human readable and electronic form suitable for inspection, review, and copying by the agency. ***GAMP Interpretation:*** *ER/ES systems should allow electronic data to be accessed in human readable form.* *ER/ES systems need ability to export data and any supporting regulatory information (e.g. audit trails, configuration information relating to identification of status of users and equipment)*  	Documents which can be generated in the frame of automated production systems after validation in RUN Time mode are: Production events and reports • Critical production parameters monitoring... • Alarms and events that can impact product quality IDS provides a wide variety of functions to: • Collect data and events generated by Vijeo Designer™ • Transfer and store them safely to a predefined IP address directory • Make them easily readable without possibility of edition therefore corruption through IDS explorer to a wide variety of users • Make them available through readable and encrypted in final storage under respective inviolability files format • Documentation and change control of application software **Those documents** are available through Vijeo Designer™ in both readable and electronic format.

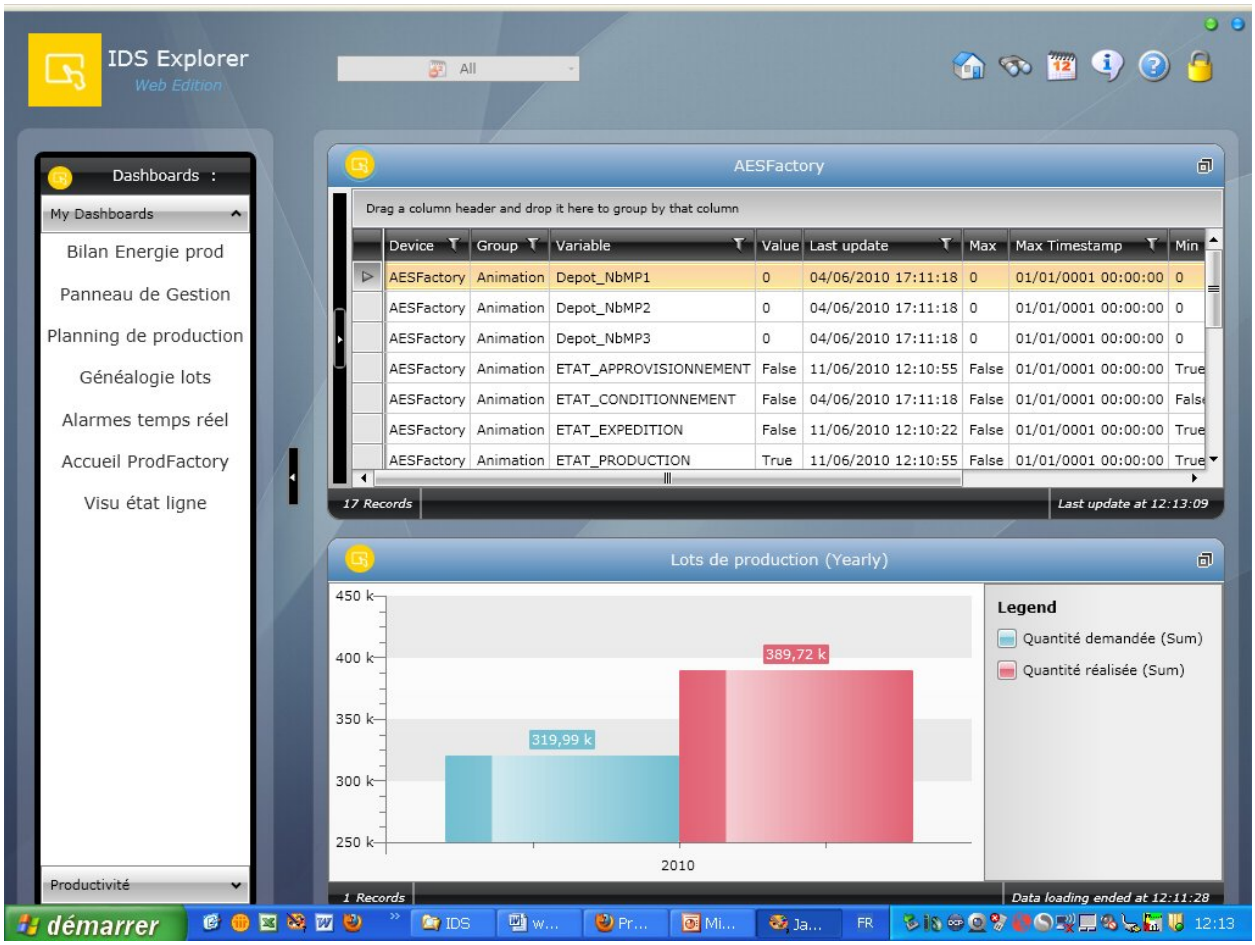
11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout retention period ***GAMP Interpretation:*** *Pharmaceutical organizations need a defined procedure for maintaining the records throughout the retention period*	Industrial from regulated industries shall define archiving periods complying with requirements in their specific field. For instance batch files shall be retained until expiry date + One year or at least 5 years. Corresponding procedures and methods for archives will be defined in the frame of QA cGMP system. IDS will allow easy retrieval and storage of consecutive version of Vijeo Designer™ software. Productys is committed to maintain compatibility of successive release of IDS in order to allow for Data availability along the life cycle.
	GAMP Interpretation: *ER/ES systems should be able to maintain electronic data over periods many years regardless of upgrades to the software and operating environment*	Schneider Electric insure compatibility of successive versions of its programs. Customers will select records formats to insure their easy retrieval along legal retention period.



Section n°	**Rule**	MAGELIS™ / Vijeo Designer™ / IDS
11.10	**Controls for closed systems**	
11.10 (d)	**Limiting system access** to authorized individuals ***GAMP Interpretation:*** *ER/ES systems should restrict access in accordance with pre-configured rules that can be maintained. Any changes to the rules should be recorded*	It is recommended that for application running with Vijeo Designer™, datas will be retrieved and stored with IDS during operation from a run time application and will be stored at any suitable location. Database can be either SQL server or IDV (Intelligent Data Vault). IDV is recommended for 21CFR part 11 applications. It is the responsibility of users to define policies to avoid uncontrolled access to these locations. Furthermore IDS Explorer provides 3 levels of access to the datas: • Public • Users • Administrator But datas are not edited through the explorer and consequently it is not possible that any of the person accessing them through the explorer would modify them. In addition Vijeo Designer™ has module security access functionality. This module prevents modifications on application programs from employees not owning sufficient access level. Therefore organization that should comply to the predicate rules have all necessary tools to implement their change control and re-validation policies safely. It is recommended to activate security module and implement associated procedures. Security access module allows for a great flexibility of levels which are sufficient for any organisation. It is generally recommended to : 1. Name an administrator for Vijeo Designer™ systems access in charge of : o User's ID definition o Attribution of rights o Follow-up of related procedures o updating 2. Realise risk analysis to determine parameters which will be protected and parameters which may be modified from interface by operators without process risk. It is recommended to limit parameters which may be modified through operating interface..

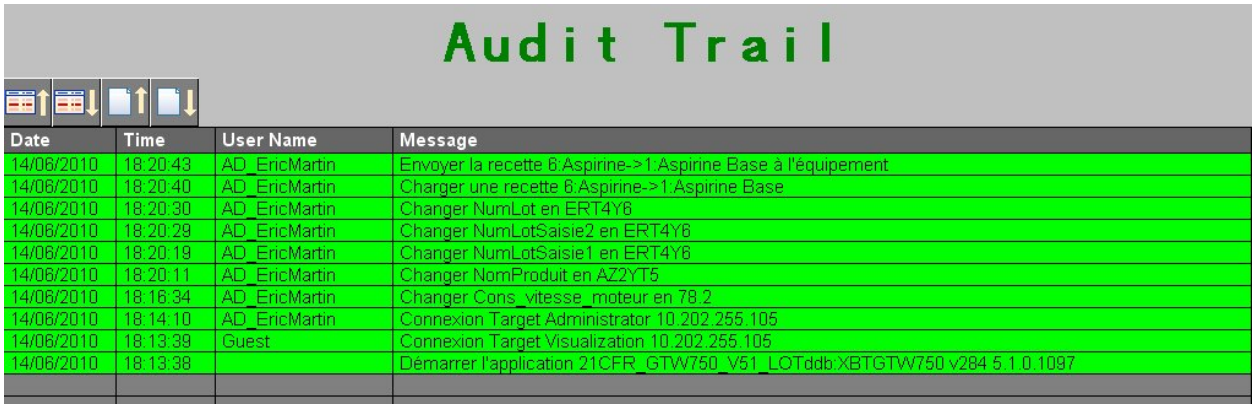
		In the event workstations or laptops are used in a non-network environment, it is recommended that Windows (version) operating system be used on these systems. The local administrator should implement unique user accounts with policies on password aging, minimum password length, password uniqueness, and account lockout after a reasonable number of unsuccessful login attempts.

Section n°	**Rule**	MAGELIS™ / Vijeo Designer™ / IDS
11.10	**Controls for closed systems**	
(11.10d) (cont.)		After software completion and process validation it is recommended to secure access and implement rules to prevent uncontrolled HMI application modification/ corruption. It is recommended to use Vijeo Designer™ functionality to: • Desactivate web access possibility • Strictly limit IP addresses allowed to access HMI
		In order to limit open session access time, screen saver maybe configured and protected by a password.



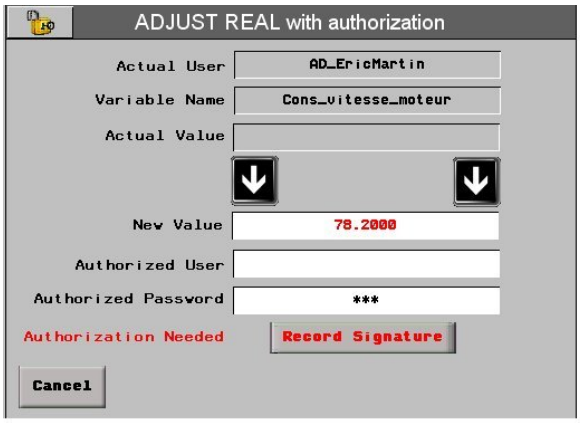
Section n°	Rule	MAGELIS™ / Vijeo Designer™ / IDS
11.10	**Controls for closed systems**	
11.10 (e)	**Use of secure, computer generated, time stamped** audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. ***GAMP Interpretation:*** *ER/ES systems should be capable of recording all electronic record create update and delete operations. Data to be recorded must include as a minimum time and date, unambiguous description of event, and identity of operator. This record should be secure from subsequent unauthorized alteration*	Vijeo Designer audit trail associated with IDS allow for full traceability of events such as • login onto the system • Signature • Set points or parameters modifications Any events recorded is date stamped. Users can use IDS to export datas and prepare dashboards that could be used as Electronic Records as per the regulatory agency definition. Datas are date stamped through file names automatic definition, that includes clearly dates and time of datas transfer. This allows for fully trace datas that are transferred. Files are transferred and stored

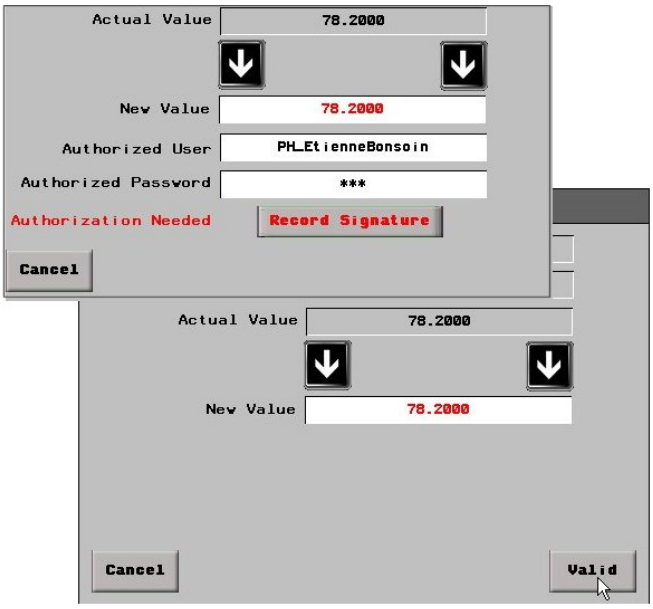
		with an encrypted copy. In order to avoid that any unidentified modification to the genuine datas is realised we recommend: 1. To implement domains security (for instance windows) to access datas storage locations. 2. To generate a periodic comparison between data files and their encrypted copys. Last generation should erase the previous one. 3. To implement a procedure of systematic comparison of files and their encrypted copies when exporting/printing/ inspecting these datas.



Section n°	**Rule**	MAGELIS™ / Vijeo Designer™ / IDS
11.10	**Controls for closed systems**	
11.10 (e)	**Records 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.	Procedures required to save and protect records resulting from audit trail implementation using IDS shall be undertaken by users. In order to facilitate retrieval of records under readable formats along retention period Schneider does advise .txt files. IDS provides such files format.
11.10 (f)	Use of operational checks to enforce permitted sequencing of steps and events as appropriate ***GAMP Interpretation:*** *Where operations are required in a pre-defined order for example in batch manufacturing the ER/ES system should enforce that sequence through the system design*	Software development will for that item follow-up Users Requirements Specification which shall take into account enforcement of sequencing steps.

11.10 (g)	Use of authority check to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device ***GAMP Interpretation:*** *ER/ES systems should restrict use of system functions and features in accordance with pre-configured rules that can be maintained. Any changes to the rule shall be recorded*	In order to meet the authority checks requirement of the rule, customers must employ policies and procedures to verify the identity of the individual to whom an electronic signature will be issued.
11.10 (h)	Use of device (e.g. terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	To ensure the validity of the source of data input, customers must ensure that all workstations are placed in secure locations and that access to the workstations is limited to authorized personnel. Vijeo Designer™ auto-check the status of running systems and the datas transferred and validates them through a signal.





Section n°	**Rule**	MAGELIS™ / Vijeo Designer™ / IDS
11.10	**Controls for closed systems**	
11.10 (i)	Determination that persons who develop maintain, or use ER/ES systems have the education training and experience to perform their assigned tasks	Training shall be forecasted for : 1. Employees involved in maintenance and development of Vijeo Designer™ applications and IDS 2. Employees accessing and operating the Datas storage work stations Employees operating computerized systems are usually trained according to customers internal training procedures or by integrators. For employees developing and maintaining Vijeo Designer™ associated with IDS applications Schneider Electric provides a wide variety of training program . Training catalogue is available on internet. Contact local vendors. Schneider Electric is recognized as being certified professional training company as such hit is entitled to issue training certificates and evaluation which is possible to use to document training of customer's operators. It is reminded that in the frame of Installation Qualification (IQ) of computerized systems it is required to establish the documented evidence that operators developing software have suitable qualification. Schneider training certificates can ideally be used in that consideration.
11.10 (j)	The establishment 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.	Corresponding procedures and their implementation are under customers responsibility.

Section n°	**Rule**	MAGELIS™ / Vijeo Designer™ / IDS
11.10	**Controls for closed systems**	
11.10 (k)	Use of appropriate controls over systems documentation including:	
1	Adequate controls over the distribution of access to, and use of documentation for system operation and maintenance	Control of documentation distributed is done under user responsibility. However Schneider Electric provides operating and maintenance manuals for its supplies. Documentation is provided under read only format in order to prevent any alteration or modification.
2	Revision and change control procedures to maintain an audit trail that documents time sequenced development and modification of systems documentation ***GAMP Interpretation:*** Where system documentation is in electronic form, an electronic audit trail should be maintained in accordance with 11.10 e	User Change control procedure shall take into account computerized system using Vijeo Designer™ and IDS as well as the protection and access of final datas storage volumes. Audit trail as implemented shall be considered in change control procedure. It allows complete traceability of modifications of applications. In case it would be implemented early enough it could support complete traceability of application development. Modifications made on operating and maintenance manuals for equipments and software from Schneider Electric and Productys are themselves subjected to respectively internal Schneider Change control procedure and internal change control procedures of Productys. Clients can have access to Schneider's update through software update contract. Customers can maintain Schneider's documentation under paper format or implement audit trail for follow-up in the frame of their complete documentation follow-up and audit trails. Automatic update could be taken into account by customers documentation audit trail software.

Section n°	**Rule**	MAGELIS™ / Vijeo Designer™ / IDS
11.50	**Signature manifestations**	
11.50 (a)	Signed electronic records shall contain information associated with the signing that clearly indicates the following	
1	The printed name of the signer	Signature realised under Vijeo Designer™ run time application included printed names of The signer. This data is transferred and stored and can be retrieved any time from the inviolability file. Then it is at any time possible to identify electronic signature of the Vijeo Designer™ session.
2	The date and time when the signature was executed	Signature generated through Vijeo Designer™ and archived with IDS are associated with time and date.
3	The meaning (such as review, approval, responsibility or authorship) associated with the signature	There are 2 levels of signature allowed by Vijeo Designer™ which is sufficient in the frame of process operation. Level: Authorship Level: Review Level of the signature realised is related to the signature and the signature events contains the level of signature. Both information can be transferred together by IDS
11.50 (b)	The items identified in § a 1, 2 and 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 records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	Following QA procedures of Schneider Electric • Accuracy of date and time Vijeo Designer™ and IDS indications are validated. Windows allows possibility to generate and follow up complying Electronic signatures.

Section n°	Rule	MAGELIS™ / Vijeo Designer™ / IDS
11.70	**Signature / record linking**	
	Electronic signatures and hand written 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 records by ordinary means.	Electronic signatures realised with Vijeo Designer™ and treated and traced with ids will be stored under genuine files. Encrypted copies are stored with the genuine files. Periodic checking implemented will insure at any time accuracy of signatures and links to the corresponding runtime generated datas. Then it is at any time possible to identify electronic signature of the Vijeo Designer™ session. Validation of accuracy of results and efficiency of archived files will be necessary for any application developed to match with functional analysis.

Section n°	Rule	MAGELIS™ / Vijeo Designer™ / IDS
11.100	**General requirements**	
11.100 (a)	Each ES shall be unique to one individual and shall not be reused by or reassigned to anyone else	Administration for Vijeo Designer™ security module does not allow signatures reallocation.
11.100 (b)		Under customer responsibility.
11.100 (c)		idem

Section n°	**Rule**	MAGELIS™ / Vijeo Designer™ / IDS
11.200	**Electronic signature components and controls**	
11.200 (a)	Electronic signatures that are not based upon biometrics shall	
1	Employ at least two distinct identification components such as identification code and password	Configuration of access defined in access security module of Vijeo Designer™ is based on : • one ID • one password Windows security module follows same rule. However IDS does not allow individual signature identification, it is not a restriction to 21CFR part 11 compliance implementation since IDS users, whatever their level can only access to data edited that cannot be modified or corrupted.
(i)	When an individual executes a series of signings during a single continuous period of controlled system access, the 1st 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	Configuration of Vijeo Designer™ and windows access security modules require utilization of both components of signature. Responsibility for Vijeo Designer™ access and modification is complete and not shared per session which is sufficient.
(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	idem
2	Electronic signatures that are not based upon biometrics shall be used only by their genuine owners	Strict rules shall be defined by customers to avoid sharing signatures and sessions access.
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 2 or more individuals	Vijeo Designer™ security module utilisation insures that only owner of electronic signature can use it

Section n°	**Rule**	MAGELIS™ / Vijeo Designer™ / IDS
11.300	**Controls for identification codes/ passwords**	
11.300 (a)	Maintaining the uniqueness of each combined identification code and password such that no two individuals have the same combination of identification and password	It is not possible neither with Vijeo Designer™ nor windows access security module to implement same combination of ID and passwords unless they have been given same ID and share password. Customers rules shall prevent it.
11.300 (b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g. to cover such events as passwords aging)	It is possible to implement automatic recall of passwords. Customers to define their policies.
11.300 (c)		Not applicable
11.300 (d)	Use of transaction safeguards to prevent unauthorized use of passwords and or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit and as appropriate to organizational management	Customers procedures shall be implemented. For instance windows security access for ids datas storage authorized stations could be designed such a way to disable users ID rights after 3 unsuccessful attempts of connections.