21 CFR Part 11, EudraLex Vol. 4 annex 11 for Computerized Systems – Assessment

Freelance 2016 Service Pack 1

The Production of drugs for human and veterinarian beings is one of the most critical tasks in the industrial production. High quality and accountability standards are an imperative to accomplish it. The United States Food and Drug Administration (FDA) as well as the European Medicines Agency (EMA) have a responsibility to ensure that drugs are safe and effective.

FDA’s regulations regarding proper manufacturing and record keeping is known as the current Good Manufacturing Practices (cGMP). Originally paper based, the record keeping moved into computerized systems. In a joint task force of industry and FDA was formed and requirement to eventually fully replace paper based records by electronic recording. In 1997 the US Federal Law directive 21 CFR Part 11 were put into place to assure, that electronic records are trustworthy as signing paper.

This rule applies to all products manufactured in the United States, and also to products manufactured elsewhere but distributed in the United States, which gives it international relevance.

In 2011 the European Union issued a regulation called EudraLex – Vol. 4 – Good Manufacturing Practice (GMP). In its annex 11: computerized systems almost equivalent requirements are described.

Applying cGMP is predominantly the duty of the end user, however it is certainly relevant as to how much a process control system supports it through technical controls. By using a process control system designed to meet these regulations, providing functionality as a COTS (commercially-off-the-shelf), the user will always benefit from less integration and validation effort and over lifetime with easier maintenance and better (or at all!) life cycle support.

Next to technical controls to achieve compliance there are procedural controls usually laid out in SOPs (Standard Operating Procedures) by the manufacturer.

1 Purpose of this whitepaper

This whitepaper will give insights on how the ABB process control systems provide off-the-shelf support for related electronic records to help you best to achieve a cGMP compliant production in a digital world. ABB’s Process control Systems as there are namely System 800xA and Freelance can be used in several combinations and support cGMP compliant production in different ways, but all of them with a maximum of off-the-shelf functionality.
2 GMP supporting Technical Controls

ABB distributed control systems (DCS) support compliance with features like system security, secure data management and reporting, electronic records and signatures, and the automated electronic recording of changes.

Core system functions that support regulatory requirements are:

- Access control
- Authentication
- Alarm and event management
- Audit trail
- Batch control and management
- Electronic recording
- Electronic signatures
- Event reports
- History and archiving
- Trends
- Redundancy
- Sequential function charts
- Shift, production and batch reports
- Infrastructure and network security

2.1 Limiting system access to authorized individuals

Our technology combines the efficiency of electronic record keeping with the security of authenticated electronic signatures.

System, engineering, manufacturing and product data are protected throughout the system’s life cycle from unauthorized access, modification or deletion in order to ensure accuracy, consistency, and completeness.

Human Interaction with our Process Control Systems are based on genuine System software packages and/or Microsoft® Windows security system and extend it to meet the demands of automation applications for life sciences industries.

System integrity can be supervised by genuine system check software (e.g. DigiCheck or My Control System – Fingerprint service).

Procedural integrity can be implied using ABB’s genuine Sequences and Batch Management software. This provides highest quality assurance and avoids human errors.
Procedural controls to limit physical access are the responsibility of the user.

ABB’s system security functions support these procedures and allow many combinations of individual users and user groups. User roles may include general permissions for administration, configuration, tuning and operation, or specific permissions for security configuration.

For login and authentication the built-in access control denies unauthorized actions. Access can be controlled from the system level down to the object level (for example a single valve or a range of cleaning equipment or an entire ingredient list). Access to functional inputs can be limited, including the right to open a single valve, or start a CIP process, or schedule the next batches and campaigns.

Operators must identify themselves at login with user name and password or biometric devices (if applicable and compatible).

In addition to authority checks, the system gives control over which changes are made. System users can be held accountable and responsible for actions initiated. The system records any operator changes made to it or to devices and applications. Time-stamped audit trails show managers as well as inspectors:
- When changes were made
- Which changes were made
- Who made the changes
- Why the changes are made

**Operational efficiency**

You can reduce data error, enhance process control, and improve data recording by replacing obsolete or inefficient equipment with automated ABB Process Control Systems technology. Introducing a process control system with integrated information management will support compliance and help reduce paperwork.

ABB Process Control Systems’ human-system interface terminals can operate as integrated control system interface, or can serve as the central operation and record keeping system coordinating connected programmable logic controllers.

A single click of the right-hand mouse button accesses further information about a signal, a mixing motor, a plant component or any other “object.” Depending on the clicked object different options are provided pre-configured as well as user defined e.g.:
- Overview Display
- System display
- Alarm and event display
- Faceplates to operate and control the tags and I/O points
- Control aspect for accessing detailed information about control logic
- Reference to various displays and logs like graphic and trend displays or signal sequence logs
- Possibly link to related SOP
ABB’s Process control Systems can enforce permitted sequencing of steps and events, as applicable. Sequential function charts offer a graphical method of organizing the control logic and manufacturing steps. Transitions are used to move from one step to the next; assigned actions are automatically initiated and interlocks are automatically monitored.

All operator actions are automatically logged into the audit trail.

By replacing paper records by electronic batch records, manufacturers are able to keep an accurate history and save huge amounts of paper records. You also gain a further method of sequencing steps and increase consistency from batch to batch.

There are several batch management packages offered with different levels of support for recipe management.

Another GMP supporting element is the in-build alarm and event management. Audible and visible alarms will enable the operator or initiate automated actions to quickly correct out-of-tolerance conditions. For example, the system will alarm in the event a low water level is reached if this had been determined to be critical parameter for the process.

The alarm and event management is system-wide and incorporates complete audit trail functionality. Alarms are typically generated when an object has an abnormal state; they are messages that the operator has to acknowledge. Events inform operators about changes and interactions. All alarms and events can be automatically logged.

The integrated audit trail let authorized users view and filter all operator actions and all events of the applications and the system. All audit trail events are time-stamped and contain additional information of the origin like tag, device identification, the change itself or the action’s owner.

The access to, and use of documentation for system operation and maintenance is outlined in 21 CFR Part 11.

Online help is part of our system, and includes guidance on configuration, operation, field device and asset management, and batch control or information management. All ABB documentation is fully version controlled in accordance with our quality procedure.

2.2 Record protection and retrieval

Archiving is a further requirement of 21 CFR Part 11. ABB’s Process Control Systems allow users to archive process data and system configuration, as well as standard operation procedures. The historian functions collect, store and retrieve historical product, manufacturing, process, batch or audit trail data. Reporting is easy. Reports present recorded data in human readable form.

The computer-generated records can be printed out, for example:

- process data records listing the times, temperatures, pressures, and other critical factors
- alarm records, listing alarm events and violations of alarm conditions noted during the process

Regular or daily audit trail reports, shift or batch reports can be scheduled using preconfigured templates. The Freelance system infrastructure ensures accuracy, reliability, integrity and confidentiality of inputs and outputs. The network is based on TCP/IP over Ethernet and utilizes built-in error detection mechanisms. Supported fieldbus standards include communication and data security mechanisms. The network also supports the operation of devices from different manufacturers. Redundant network communications are supported for all communication levels.
The whole system, including communication design and network security, is verified against the development and system requirements in accordance with ABB’s quality procedures.

Tests are applied to individual modules and to the entire system. The system is also designed and tested against the customer’s specific needs.

We develop automation technology that meets validation and regulatory requirements. Compliant solutions are delivered and supported by our validation and compliance professionals, ensuring seamless integration into regulated and quality controlled processes.

2.3 Professional skills

Automation systems are becoming increasingly essential to pharmaceutical production. Whether our control products are embedded in process equipment or function as a stand-alone system, they are critical to achieving product quality. Our unique integration of 21 CFR Part 11 support into our technology makes it easy to build compliant applications.

Are your quality assurance and validation managers under pressure to deliver greater assurance with smaller teams? Do they increasingly rely on the active support of other parts of the organization and suppliers to meet regulatory needs?

ABB offers an excellent capability in the validation of all computer systems. With our considerable track record in managing automation technologies and projects, we can deliver both regulatory compliance and optimal business benefit.

We are known for flexibility in our approach. Our specialists are experienced practitioners who have dealt with issues similar to those you currently face. Building on this hands-on experience and our knowledge of regulatory needs, we can help you to understand and manage your validation issues.

3 Concerned System and Software

<table>
<thead>
<tr>
<th>System name</th>
<th>Freelance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>2016 SP1</td>
</tr>
<tr>
<td>Deliverables</td>
<td>Freelance 2016 SP1 with following deliverables</td>
</tr>
<tr>
<td></td>
<td>- Freelance Engineering (formerly DigiTool, Control Builder F)</td>
</tr>
<tr>
<td></td>
<td>- Freelance Operations (formerly DigiVis)</td>
</tr>
<tr>
<td></td>
<td>- Security Lock (formerly DigiLock)</td>
</tr>
<tr>
<td></td>
<td>- Archive Browser (formerly DigiBrowse)</td>
</tr>
<tr>
<td></td>
<td>- Process station types: AC 700F, AC 800F, AC 900F</td>
</tr>
<tr>
<td></td>
<td>- Freelance Formulation Version 1.2</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>ABB Inc.</td>
</tr>
<tr>
<td>Supplier</td>
<td>ABB Inc.</td>
</tr>
</tbody>
</table>
## Part 11 Requirements

### Subpart B – Electronic Records

#### Sec. 11.10 Controls for closed systems.

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

- **(a)** Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.
- **(b)** The ability to generate accurate and complete copies of record in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

### Engineering and Application Management

The end-user and manufacturer is responsible for developing procedures to support automation applications in regulated environments. Our validation experts support a full spectrum of compliancy efforts, including end-user validation, SOP development and risk-based approaches to dealing with 21 CFR Part 11 issues.

- Configuration files can be printed as they are and easily be checked. Alterations will be shown in the engineering tool wherever the changes impact the configuration. Customer must take care of an audit trail by either by taking copies or use version tracking tools.

### Operations and Runtime

The end-user and manufacturer is responsible for developing procedures to support automation applications in regulated environments. Our validation experts support a full spectrum of compliancy efforts, including end-user validation, SOP development and risk-based approaches to dealing with 21 CFR Part 11 issues.

- All operator actions, alarm/events, user log on/off events, Batch events, batch states and TTD (time tagged data) are storable in non-editable records. Batch reports are saved on the batch server and cannot be altered. Records from Freelance Operations can be exported and converted to CSV files (ASCII readable files) producing copies.

Furthermore all records are stored in Windows files and as such can be copied.
<table>
<thead>
<tr>
<th>Part 11 Requirements</th>
<th>Engineering and Application Management</th>
<th>Operations and Runtime</th>
</tr>
</thead>
</table>
| (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period. | Configuration can be protected by password managed by Freelance security tool.  
Configuration is auto-stored and can easily be backed up and restored.  
Customer should have policies to manage base lines and password management | Freelance Operations in conjunction with Archive Browser and Formulation provides historical data archiving to removable media such as Optical Disk for long term storage. Through appropriate procedure, the user must ensure that the archiving feature is properly configured and that removable media are inserted and replaced as the media space is allocated. |
| (d) Limiting system access to authorized individuals. | Configuration can be protected by password managed by Freelance security tool.  
As of Freelance 2019 full MS Windows access control capability including Auto-Log out can be applied | Freelance Operations, SecurityLock and Formulation provide a consistent layered security. A policy needs to be maintained by the user to manage the users and user groups  
Extended security features are provided by Freelance 2019 and System 800xA Operations |
| (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. | Not applicable | Audit trail is supported via System log. Freelance Operation and Freelance Formulation provide operator action logging with user name, timestamp, pre-change and post change values. All logged events are appended to the historical log such that all events remain permanently stored and can easily be sent to a central logging server.  
Each operator action is stored with area, time-stamp, user name, object name, component, old value, new value and dimension. 800xA Operations offers in addition a convent way to utilize dual signature, comments and reasoning of the action  
The event log and the audit trail file is limited but can easily be filed in a binary format. A Windows message will be generated in the case of a full log file.  
Event-Log must be set to not overwrite previous records. |
<table>
<thead>
<tr>
<th>Part 11 Requirements</th>
<th>Engineering and Application Management</th>
<th>Operations and Runtime</th>
</tr>
</thead>
<tbody>
<tr>
<td>(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.</td>
<td>Engineering allows for sequencing and recipe management to assure sequences to be followed accurately. Sequences and Recipe execution can be limited to groups or individual operators. Operation can be limited on a tag level.</td>
<td>Freelance Operations supports a Sequential Function Chart display which allows operation of SFC program. Freelance Formulation allows Recipe and Parameter Management to have restricted (view only) mode. Operator Actions are per default to be confirmed by a Two Step “Select – Apply” control and can be restricted on a tag level</td>
</tr>
<tr>
<td>(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.</td>
<td>Configuration can be protected by password managed by Freelance security tool. As of Freelance 2019 full MS Windows access control capability including Auto-Log out can be applied.</td>
<td>Freelance Operation and Freelance Formulation utilize user access management down to the individual tag. User can be managed in groups to assign the different policies. Freelance Operations and Freelance Formulation does not allow a double signature per default, individual engineering or an SOP would be required. Alternatively the use of 800xA Operations instead of Freelance Operations should be considered.</td>
</tr>
<tr>
<td>(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.</td>
<td>Data entry requires Freelance software to be properly installed, which can easily be checked with genuine Freelance tools.</td>
<td>Access rights for a user are operator station specific. The same user can be assigned a different profile on different operator stations. Thereby it is possible to make sure that certain operations are only executed from a specific operator station.</td>
</tr>
<tr>
<td>(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.</td>
<td>ABB provides customer training with documentation and certification. Users need to ensure, that personnel is properly trained. Freelance provides soft controllers (emulator) to easily train engineers and operators offline.</td>
<td>ABB provides customer training with documentation and certification. Users need to ensure, that personnel is properly trained</td>
</tr>
</tbody>
</table>
### Part 11 Requirements

#### Engineering and Application Management

- **(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.  
  - User must establish policies to adhere

- **(k)** Use of appropriate controls over systems documentation including:  
  1. Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.  
  2. Revision and change control procedures to maintain an audit trail that documents time-sequence development and modification of systems documentation.  
  - Freelance Engineering documents the configuration of the entire system in a graphical way as is by few clicks.  
  - The project related documentation needs to be maintained by 3rd party tools, ABB can offer consultancy of which can be used best.  
  - 3rd party software like AUVESY versiondog can help creating a digital version management  
  - ABB maintains any of its system documentations by a document management system to assure its life cycle and proper versioning.

### Sec. 11.30 Controls for open systems.

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

<table>
<thead>
<tr>
<th>Part 11 Requirements</th>
<th>Engineering and Application Management</th>
<th>Operations and Runtime</th>
</tr>
</thead>
<tbody>
<tr>
<td>(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.</td>
<td>User must establish policies to adhere</td>
<td>User must establish policies to adhere</td>
</tr>
<tr>
<td>(k) Use of appropriate controls over systems documentation including:</td>
<td>Freelance Engineering documents the configuration of the entire system in a graphical way as is by few clicks.</td>
<td>Each system version has its documentation of the entire system, which is consistent. Customer can get access to it.</td>
</tr>
<tr>
<td>Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.</td>
<td>The project related documentation needs to be maintained by 3rd party tools, ABB can offer consultancy of which can be used best.</td>
<td>ABB maintains any of its system documentations by a document management system to assure its life cycle and proper versioning.</td>
</tr>
<tr>
<td>Revision and change control procedures to maintain an audit trail that documents time-sequence development and modification of systems documentation.</td>
<td>3rd party software like AUVESY versiondog can help creating a digital version management</td>
<td></td>
</tr>
<tr>
<td>Sec. 11.30 Controls for open systems.</td>
<td>n/a Freelance is a closed system</td>
<td>n/a Freelance is a closed system</td>
</tr>
</tbody>
</table>
### Part 11 Requirements

<table>
<thead>
<tr>
<th>Sec. 11.50 Signature manifestations.</th>
<th>Engineering and Application Management</th>
<th>Operations and Runtime</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:</td>
<td>Freelance Engineering cannot be digitally signed. This must be provided by 3rd party tools. However – Freelance Engineering can digitally print out the full system and application configuration or only parts at any time to the full content by just few clicks, which then can be digitally signed by a 3rd party tool.</td>
<td>Freelance Operations stores operator actions, such as “setpoint changed by” area, time-stamp, user name, object name, component, old value, new value and dimension. Comments and reasoning have to be configured in an application. A full digital support of this section is provided using Freelance with 800xA Operations and 800xA Batch</td>
</tr>
<tr>
<td>(1) The printed name of the signer;</td>
<td>n/a</td>
<td>ABB products provide database security to ensure validity of records. Operator Audit trails are stored in a binary format and cannot be edited. A service program translates it into human readable format, which is read only</td>
</tr>
<tr>
<td>(2) The date and time when the signature was executed;</td>
<td>Freelance Engineering by system design does not allow for alteration of any log or historian file.</td>
<td>The administration user must configure system user access such that user access is limited to standard interfaces.</td>
</tr>
<tr>
<td>(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).</td>
<td>Printed reports are typically formatted by the user and thus require proper configuration such that printed records display complete records including user name, timestamp, identification of changed object, pre-change and post-change values</td>
<td></td>
</tr>
</tbody>
</table>

### 1. Subpart C – Electronic Signatures

<table>
<thead>
<tr>
<th>Sec. 11.100 General requirements.</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.</td>
<td>User is responsible to assure, that operators have a unique user name and password. Freelance security lock allows for 16 user groups and 1000 individual users per installed system. As of Freelance Version 2019 user management allows to apply all MS Windows policies.</td>
<td>User is responsible to assure, that operators have a unique user name and password. Freelance security lock allows for 16 user groups and 1000 individual users per installed system. As of Freelance Version 2019 user management allows to apply all MS Windows policies.</td>
</tr>
</tbody>
</table>
### Part 11 Requirements

#### Engineering and Application Management

(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.

Procedural controls must be established to assure, that user name and password matches individual system users

(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

1. The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.

2. Persons using electronic signatures shall, upon agency request provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer’s handwritten signature.

Sec. 11.200 Electronic signature components and controls.

(a) Electronic signatures that are not based upon biometrics shall:

1. Employ at least two distinct identification components such as an identification code and password.

Freelance security lock implies user name and password to be required to use the system. Policies may be applied. As of Freelance Version 2019 all MS Windows policies can be applied including password aging.

Passwords are never displayed and are not accessible by any user

Freelance security lock implies user name and password to be required to use the system. Policies may be applied. As of Freelance Version 2019 all MS Windows policies can be applied including password aging.

Passwords are never displayed and are not accessible by any user