Life sciences solutions

compliant with FDA 21 CFR Part 11

- Improving operational efficiency, productivity and quality for better outcomes

ABB Ability 800xA makes compliance easy, while also providing opportunities to lower production cost, consume less energy, produce less waste and make continuous quality improvements. More control plus better data – for more informed decision-making, more efficient and compliant operations.

System 800xA facilitates regulatory compliance

As part of ABB's strategy we have invested considerably in the development of advanced solutions and services in the life sciences industries.

One of the most important regulations relevant to pharmaceutical manufacturing is 21 CFR Part 11, issued by the U.S. Food and Drug Administration. This rule applies to all products manufactured in the United States, and to products manufactured elsewhere but distributed in the United States, which gives it international relevance.

21 CFR Part 11 has two main areas of enforcement: electronic records and electronic signatures. Moving to a paperless world with fully electronic data handling promises cost savings from improved efficiency and reduced physical handling and storage. Electronic signatures are given legal equivalence with traditional "wet ink" signatures on paper.

In life sciences companies, 21 CFR Part 11 is applied to automation or computer system applications that manage product-related data such as:

- Calibration and maintenance
- Cleaning automation
- Corrective actions
- Critical equipment and instrumentation
- Facility and building automation
- HVAC controls and alarm handling
- Manufacturing instructions
- Material traceability
- Recipes and formulations
- Packaging automation and labeling information
- Security access control

Extended Automation System 800xA facilitates compliance with the rule 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 and re-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

System 800xA makes automation and regulatory compliance easy.

Limiting system access to authorized individuals

System 800xA automation technology facilitates compliance with FDA 21 CFR Part 11 and integrates electronic records and electronic signatures as core system functions.

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 to ensure accuracy, consistency, and completeness. We utilize the Microsoft® security system and extend it to meet the demands of automation applications for life sciences industries.

Users and user roles
Standard procedures to limit physical access are the responsibility of the pharmaceutical company. 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 and for first and second digital signature.

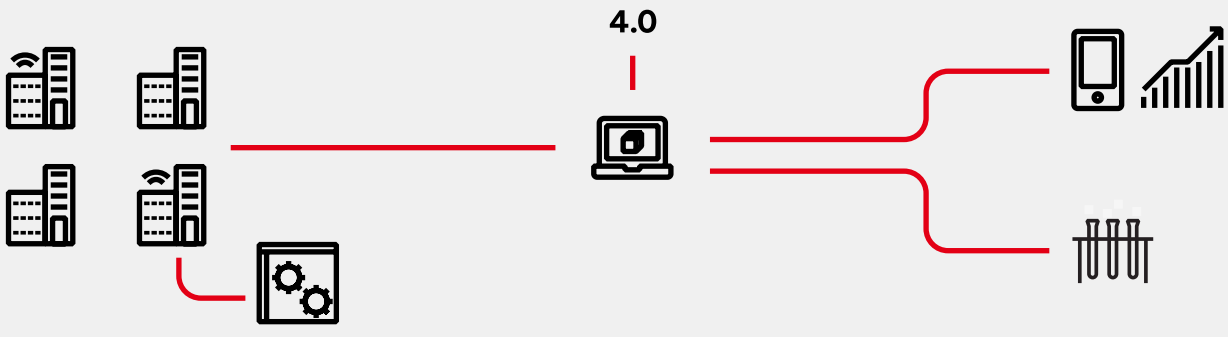
Access control
For login, authentication and electronic signing, two component security codes apply. Every combination of user identification and password is unique. Minimum password length, password aging, and rules against re-using recent passwords are all configurable.

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 both at login and before an input is accepted; for example, before a motor is switched on or a cleaning process is started.

Change control
In addition to authority checks, the system gives pharmaceutical manufacturers control over which changes are made. Using electronic signatures, system users can be held accountable and responsible for actions initiated. This could apply, for example, to the configuration of control applications, including all embedded logic and I/O functions for release to production.

The system records any 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, and why

System 800xA makes automation secure, and tracks changes automatically.



Operational efficiency

You can reduce data error, enhance process control, and improve data recording by replacing obsolete or inefficient equipment with automated 800xA technology. The introduction of a new control system with integrated information management will facilitate compliance and help reduce paperwork.

Relevant information at your fingertips
800xA 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." The information, called aspect, is connected to the object and includes:

- Graphic displays with real-time data from your process
- Faceplates to operate and control the tags and I/O points
- Pre-configured trend displays
- Alarm and event displays
- Trend, alarm and event history
- Device calibration history
- Online help

Sequencing of steps
System 800xA 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.

Manufacturing instructions
System 800xA improves security through operational checks also for manual operations. Manufacturers can replace paper records by online instruction sheets, a proactive way to ensure the sequencing of steps to be taken.

The operators follow the interactive operation procedures or instructions line-by-line, supported by the system. All operator actions are automatically logged into the system audit trail. For critical settings, re-authorization can be mandated before the system will accept the change.

Electronic batch records
By replacing paper records by electronic 800xA 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.

System integrated 800xA Batch Management is built to ISA S88 standards. Batch procedures describe how pharmaceutical products are manufactured.

Information on the status of process and batch operations is easily accessible through integrated batch scheduling, control and reporting features. Batch and signature events are an integrated part of the system audit trail.

Consistent performance

Alarm and event management
On the technical side, 800xA alarm and event management is another compliance element to ensure consistent intended performance. 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 from the thermal processing stand point. 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 must acknowledge. Events inform operators about changes and interactions. All alarms and events can be automatically logged into the historian.

Audit trail
The integrated system-wide audit trail lets authorized users view and filter:
- User login, logout and change events
- Configuration changes
- Operator actions and inputs
- Alarm events
- System and device events
- Calibration alarms and events
- Batch alarms and events
- Signature events

All time-stamped audit trail events contain information about the object or file changed, the change itself and the action's owner. System 800xA also logs the reasons for the change and optional comments that the user has entered.

Electronic signatures
Critical operations in a process or critical changes of machine settings might require significant authentication steps to ensure that the correct persons have the rights and authority to perform certain actions. Pharmaceutical manufacturers who decide to use additional security checks before users are allowed to download setpoints or issue commands rely on the 800xA human-system interface. The user will be required to provide username, password and new value and, if necessary, comments or a supervisor signature before the change affects the process.

Documented
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.

Record protection and retrieval

Archiving
Archiving is a further requirement of 21 CFR Part 11. System 800xA allows users to archive process data and system configuration, as well as standard operation procedures.

History and reporting
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, calibration or batch reports can be scheduled using preconfigured templates. Templates can also be customized in the familiar Microsoft Windows® desktop. ODBC, OLE DB and SQL provide additional access to the archive. Full 21 CFR Part 11 support applies to the all historian functions, such as access control, electronic signing of reports, data protection and integrity.

Infrastructure
The 800xA 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.

Quality assurance
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, such as 21 CFR Part 11 support. We develop automation technology that fully 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.

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.

Freedom of choice
Our 800xA technology offers you a faster path to manufacturing efficiency. Take advantage of system 800xA and choose the functional area you need, without concerns about compliance. All our products — visualization, batch or information management, maintenance, fieldbus devices, maintenance and calibration integration, or package unit and OPC server connectivity — come with built-in 21 CFR Part 11 support. They all use the same system security features, offer the same authorization and signature support, and log events to the same audit trail.

An experienced validation partner
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 industry leading 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.

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. We are known for flexibility in our approach. We are able to cover in depth all aspects of regulatory compliance from R&D (laboratories and LIMS) to production (facilities and process equipment), business systems (MRPII and MES) and warehouses.

Your IT partner
ABB is more than an equipment and automation provider. We are your complete industrial information technology partner. Changing market demands require faster turnarounds, greater customization, smaller lot sizes, and lower overall costs. With Extended Automation System 800xA, ABB provides you with the technology to extend productivity gains by:

- Fully integrated FDA 21 CFR Part 11 support
- Delivering control and I/O to meet entire plant needs
- Optimizing plant asset availability and performance
- Improving batch consistency, quality and cycle time
- Integrating information for improved visibility

21 CFR Part 11 checklist

Our automation technology addresses your 21 CFR Part 11 requirements. This initial checklist for closed system introduces our system support. The assessment compares the actual regulation test with typical compliant implementation examples using the ABB automation system.

Section	21 CFR Part 11 Regulation Text	ABB Implementation and Application
B-11.10	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:	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.
(a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Our customers need to validate their installation. We help by providing project execution and product development methodologies that integrate validation activities throughout the system development life cycle. ABB's automation system supports access control. It registers changes to electronic records as audit trail events. It can be configured to check the validity of input data.
(b)	The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	Configuration as well as production data, like recorded history, audit trails or batch reports, can be exported or archived. The information is available online to the authorized operator in either standard or customized displays, or can be printed or exported.
(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Our experts help our customers fulfill business and regulatory drivers associated with record retention by defining appropriate procedures for access, archival and retrieval of records. Our automation system supports long-term archiving.
(d)	Limiting system access to authorized individuals.	Standard procedures to limit physical access are the responsibility of the customer. System access is managed through the use of a unique user ID and password combination for each user. Additionally, the system supports a number of schemes to prevent the compromising of a user's password including minimum password length, password ageing and preventing the re-use of recent passwords.
(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.	The audit trail is an integrated system function. In general, historical data cannot be altered. Time-stamped audit trail events detail object or file name changes, operator ID, description of change and node. If the change is subject to authorization or electronic signature, then the audit trail will also show the reason and any comment. Audit trail events can be viewed, printed and archived. Change of date and time is access controlled.

Section	21 CFR Part 11 Regulation Text	ABB Implementation and Application
(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Our automation system supports interlocks and sequential function charts. Our integrated Batch Manager is built to ISA S88 and IEC 61512 standards.
(g)	Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	The system restricts access according to the user and user role configuration. The rules relate to the use of system functions, workstations, operator actions, tags or event single tag signals. When the rules are changed, the system automatically generates an audit trail event.
(h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	The functional scope of system servers or clients is defined during system configuration. In addition, user roles and access can be limited to single or specified nodes.
(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.	The customer is responsible for ensuring that personnel working with the automation system are qualified. Under ABB's quality system, ABB trains and documents the training of ABB product and system development staff and implementation personnel.
(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.	The system owner is responsible for defining the policy for the manufacturing or production facility. Our consultants support our customers in setting up the required procedures and documents.
(k)	Use of appropriate controls over systems documentation including: • Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance • Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	The customer's organization is responsible for ensuring change control procedures for operational and maintenance documentation. Our experts are prepared to help our customers. All ABB documentation is fully version controlled in accordance with our quality procedure. Online help is part of our system. User manuals are included on the distribution media. The product documentation is delivered in PDF files.
B-11.50 (a)	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: • The printed name of the signer • The date and time when the signature was executed • The meaning (such as review, approval, responsibility, or authorship) associated with the signature	When electronic records are signed, the system records the following items as part of the electronic signing process: • Date and time stamp • User ID and full name of the signer(s) • Reason for signature, out of a preconfigured list of possible reasons • Optionally, an additional comment by the signer at run-time • PC/node, where the signature was made
(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).	The electronic record includes the signature aspect, which is stored in the same system database. The system allows us to display the electronic signature as described in 11-50 (a) either on the screen or in a report.
B-11.70	Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	The signature event, with an explanation of the status or reason (such as "approved" or "maintenance action"), is linked to the electronic record and securely archived with the record and through the audit trail.
C-11.100 (a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	The system security is based on Microsoft Windows Security. All user identification and password combinations are unique.
(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.	The customer organization is responsible for assigning access rights to operators and other users, which allow them to use our system.
(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. • 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 • 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.	Our customers are responsible for submitting a certification to the agency that the electronic signatures used in their system are intended to be the legally binding equivalent of traditional handwritten signatures.

Section	21 CFR Part 11 Regulation Text	ABB Implementation and Application
C-11.200 (a)	Electronic signatures that are not based upon biometrics shall: • Employ at least two distinct identification components such as an identification code and password	For security, our system requires two components for authorization and electronic signatures, the user identification and password.
	(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.	The system distinguishes between an electronic signature assigned and linked to an electronic record, and an authorization for controlled system access, e.g., to open a valve or to schedule a batch recipe. The user must enter his or her user ID and password for each separate signature action.
C-11.200 (a)	(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.	Each signer must identify him or herself with unique user ID and password, irrespective of the type of signature requested: 1st or 2nd signatures from an individual or a member of a user group.
	• Be used only by their genuine owners	Our customers need to set up appropriate procedures and policies.
	• Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals	The pharmaceutical organization is responsible for installing appropriate procedures and policies. Password data cannot be retrieved from the system. Security and access control limit access to electronic records and audit trail information.
(b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Our security and access controls are built around standard Microsoft security features.
C-11.300 (a)	Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: • Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	Every combination of user identification and password is unique.
(b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password ageing).	In addition to organizational procedures, the system technology supports password ageing and minimum password length and prevents the reuse of a configurable number of prior passwords.
(c)	Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	Our customer is responsible for defining procedures for handling forgotten or lost passwords. If you need help in this process, please contact ABB.
(d)	Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	The system utilizes Microsoft security, which allows the system to disable a user's account after consecutive failed logins. Failed attempts to login, authorize or electronically sign records are logged as audit trail events by the system.
(e)	Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	This is the responsibility of the system owner. Our experts can support this effort.

ABB Inc.

abb.com/life-sciences

3BHT 490781 R0001