WYATT TECHNOLOGY

WHITE PAPER

ASTRA with Security Pack and EU Annex 11

Introduction

Wyatt Technology's ASTRA® Security Pack (SP) product provides multiple features to address those aspects of regulatory compliance that are relevant to the ASTRA software in a regulated environment per Title 21/Part 11 of the U.S. Code of Federal Regulations (21 CFR Part 11). Please refer to M1008, *ASTRA SP: Security Pack for 21 CFR Part 11 compliance*, for details.

A more recent (June 2011) policy from the European Union, EU Annex 11, has a similar intent to 21 CFR Part 11 for Europe. While 21 CFR Part 11 is a federal law in the United States, EU Annex 11 is a set of strongly-recommended guidelines for Good Manufacturing Practice in the European Union.

It is important to understand ASTRA's compliance with EU Annex 11, since it does apply to any manufacturers who are seeking EU market approval. What follows below are all provisions of the EU Annex 11 guidance (printed in blue) with statements from Wyatt addressing each provision (printed in black).

While EU Annex 11 does have a larger scope relative to 21 CFR Part 11, it does not add additional software requirements that must be addressed in ASTRA. Instead, the core of EU Annex 11 puts additional responsibilities on our customers to validate suppliers, continually assess IT infrastructure, and ensure the integrity of systems at all levels on an ongoing basis. Wyatt is prepared to work closely with EU customers and other customers conforming to EU Annex 11 to address their validation needs, both before and after the sale.

ANNEX 11: COMPUTERISED SYSTEMS

Principle

This annex applies to all forms of computerised systems used as part of a GMP regulated activities. A computerised system is a set of software and hardware components which together fulfill certain functionalities.

The application should be validated; IT infrastructure should be qualified.

Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance. There should be no increase in the overall risk of the process.

General

1. Risk Management

Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.

Establishing and maintaining a robust risk management system is the responsibility of the customer.

2. Personnel

There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.

Ensuring that all personnel have appropriate qualifications, appropriate access, and defined responsibilities is the duty of the customer. Wyatt will provide training on Wyatt's systems to personnel that require it.

3. Suppliers and Service Providers

3.1 When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous.

Customers are encouraged to have an agreement with Wyatt to define Wyatt's responsibilities regarding the provision, installation, configuration, integration, maintenance, modification, and retention of Wyatt instruments, software, and systems. Creating such an agreement is the responsibility of the customer, and Wyatt will acting in partnership with the customer to produce such an agreement.

3.2 The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.

Wyatt is an ISO 9001:2015 certified manufacturer with a robust quality management system for hardware and software.

3.3 Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.

Wyatt documentation can be provided at any time for the customer to validate that it meets their user requirements.

3.4 Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.

It is the responsibility of the customer to keep quality system and audit information available to inspectors.

Project Phase

4. Validation

4.1 The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.

It is the customer's responsibility to generate the relevant validation documentation, including standard, protocols, acceptance criteria, procedures, and records.

4.2 Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.

It is the responsibility of the customer to maintain adequate documentation throughout the validation process.

4.3 An up to date listing of all relevant systems and their GMP functionality (inventory) should be available.

For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.

Maintaining an up-to-date listing of all relevant systems, their GMP functionality, and detailed arrangements of critical systems is the responsibility of the customer. Wyatt will assist with providing details on hardware pre-requisites, software pre-requisites, and relevant security measures.

4.4 User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle.

The creation and maintenance of User Requirements Specifications (URS) is the responsibility of the customer. Wyatt will work in partnership with the customer to ensure that URS requirements are addressed with Wyatt hardware and software.

4.5 The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately.

Wyatt is an ISO 9001:2015 certified manufacturer with a robust quality management system for hardware and software.

4.6 For the validation of bespoke or customised computerised systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system.

ASTRA with Security Pack is a commercial off the shelf system. We do not consider it to be a bespoke or customized computer system. This does not apply.

4.7 Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy.

Details on the relevant IQ/OQ procedures used to validate ASTRA and Wyatt Instruments can be provided to the customer.

4.8 If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.

It is the responsibility of the customer to validate that data are not altered in value or meaning when migrating data from one system to another. It is the responsibility of Wyatt to provide information on the testing of data migration to or from ASTRA and to ensure that appropriate validation code exists wherever ASTRA might import or export data.

Operational Phase

5. Data

Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.

ASTRA can import files from other chromatography software, such as Agilent OpenLab (ChemStation) and Waters Empower. These import routines include built-in checks that validate the data as it is imported. Validation checks are also completed on data that is exported from ASTRA.

6. Accuracy Checks

For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.

ASTRA does provide some validation of manually entered values. That is, if a value is outside a preset range for a particular parameter then ASTRA will not allow the value to be entered. Further, ASTRA with Security Pack will prohibit the modification of some critical experiment values if the user does not have sufficient access privileges. However, it is the responsibility of the customer to ensure that all manually entered values are accurate and appropriate for the collection or analysis that is desired.

7. Data Storage

7.1 Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period.

ASTRA with Security Pack provides electronic access control that secures data from damage or deletion. It is up to the customer to provide physical security for data. It is also the customer's responsibility to ensure regular checks of the accessibility, readability, and accuracy of the data.

7.2 Regular back-ups of all relevant data should be done. Integrity and accuracy of back- up data and the ability to restore the data should be checked during validation and monitored periodically.

ASTRA with Security Pack utilizes Microsoft SQL Server for data storage, which has robust backup capabilities. It is up to the customer to setup an appropriate backup system and maintain regular backups.

8. Printouts

8.1 It should be possible to obtain clear printed copies of electronically stored data.

ASTRA supports printing of all displayed data and reports.

8.2 For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry.

When ASTRA is used in a QC environment, the audit trail for each experiment may be printed and examined to determine what data operations were completed.

9. Audit Trails

Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.

ASTRA with Security Pack generates a complete audit trail that contains a log of all operations related to data acquisition, data storage, and data analysis. This audit trail can be exported to a text file. It will be the responsibility the customer to regularly review the audit trail.

10. Change and Configuration Management

Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.

The customer will define the appropriate procedure for changes to a computerized system.

11. Periodic evaluation

Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.

These periodic evaluations of computerized systems are completed by the customer.

12. Security

12.1 Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.

ASTRA with Security Pack uses personal codes with passwords to prevent unauthorized access. Once authenticated, the user’s actions can be limited by assigning them to one of four predefined access levels. Wyatt recommends additional physical security, such as keys or pass cards, for any GMP installation.

12.2 The extent of security controls depends on the criticality of the computerised system.

The total level of security is up to the customer. ASTRA with Security Pack provides several layers of security, but more may be required depending on the how critical the system is.

12.3 Creation, change, and cancellation of access authorization should be recorded.

ASTRA with Security Pack relies on the local Microsoft Windows domain controller to provide authentication. The administrator of that system should ensure that appropriate logging is enabled to track these changes for the customer.

12.4 Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.

All operations that have the potential to modify data or results are appropriately logged, including operator identity, the current date, and the current time.

13. Incident Management

All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.

Failure recording and analysis is the responsibility of the customer. Wyatt will work in partnership with the customer to analyze failures of a Wyatt system.

14. Electronic Signature

Electronic records may be signed electronically. Electronic signatures are expected to:

a. have the same impact as hand-written signatures within the boundaries of the company,
b. be permanently linked to their respective record,
c. include the time and date that they were applied.

ASTRA with Security Pack allows for electronic signatures that are permanently logged, including the operator, current date, and current time of the signature.

15. Batch release

When a computerised system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.

When ASTRA with Security Pack is used in a QC environment, an authorized individual may sign off on a set of results using an electronic signature.

16. Business Continuity

For the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.

The customer is responsible for ensuring that their computing infrastructure is robust against critical failures. Wyatt can provide recommendations if needed.

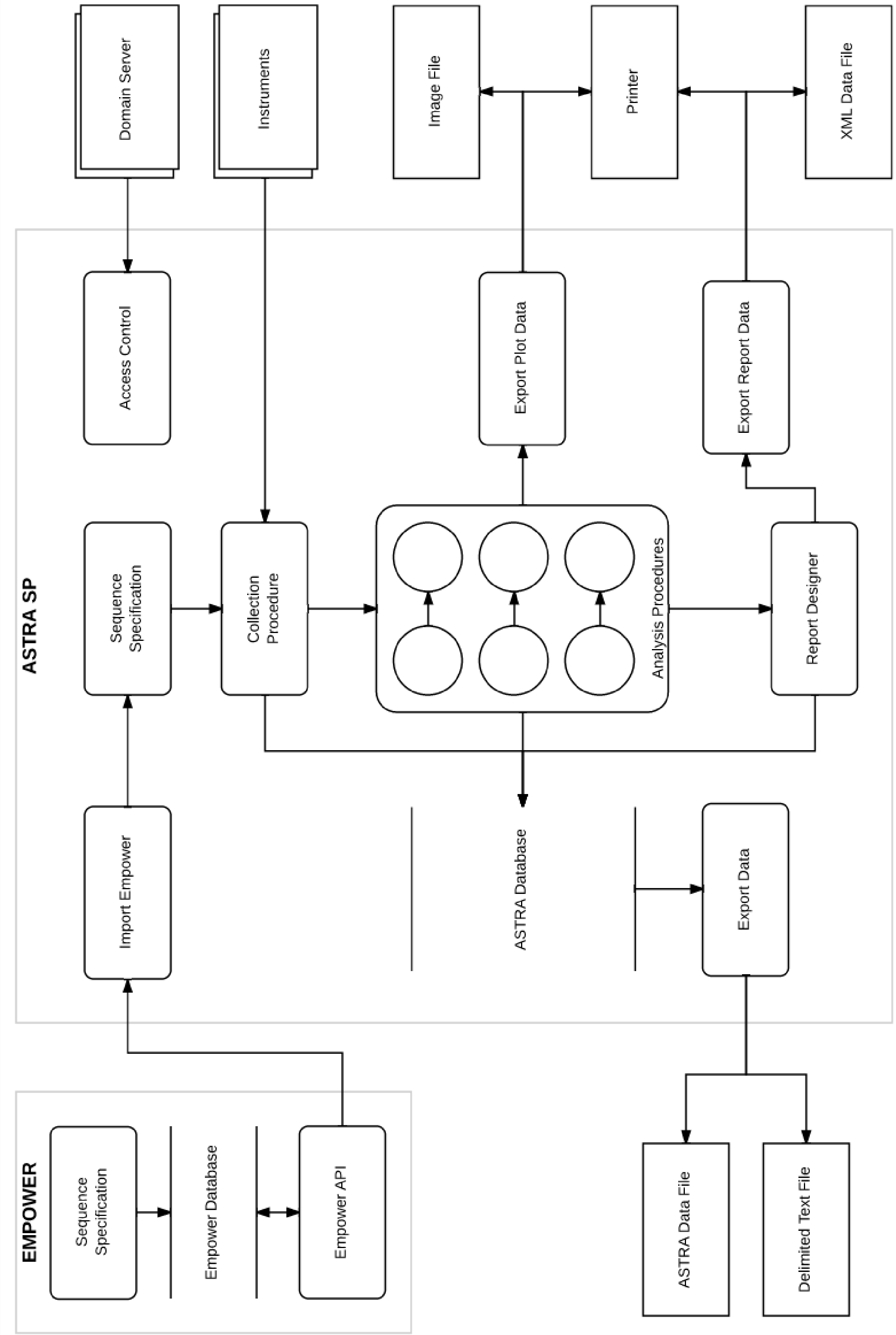
17. Archiving

Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.

The customer is responsible for ensuring adequate archives and backups of data.

ASTRA SP Data Flow

The following diagram illustrates the major data flow pathways present in ASTRA SP. It includes all inputs and outputs from the ASTRA SP application as well as an example of importing sequence information from the Empower application.


EMPOWER
Sequence Specification
Empower Database
Empower API
ASTRA SP
Import Empower
Sequence Specification
Access Control
Domain Server
Instruments
Collection Procedure
Analysis Procedures
ASTRA Database
Export Data
Export Plot Data
Image File
Printer
XML Data File
Export Report Data
Report Designer
ASTRA Data File
Delimited Text File

Questions?

Please contact us if you have any questions. If you are one of our international customers, feel free to contact your local representative directly. Contact information for our global offices is listed at www.wyatt.com/Distributors.

You may reach our corporate office at support@wyatt.com or by calling us at +1 (805) 681-9009. Selecting option 4 will connect you with our Customer Support team.

WYATT TECHNOLOGY