ID	Topic	Question	Answer
C1-1	Archive	The system must be able to archive records to alternate media for storage.	This falls within the responsibility of the IT department
C1-2	Archive	The system must be able to load archived records back into the system.	Yes
C1-3	Audit Trail	The audit trail must record any events that create, modify or delete electronic records.	Yes for data within the files. For the files themselves the windows permission must be set properly.
C1-4	Audit Trail	The system must be able to produce visual displays of audit trails of electronic record data and their associated metadata. Where the said audit trail represents a change to data, then the system must make that change clear, precise and concise in the display.	Yes
C1-5	Audit Trail	The system must be able to output electronically to a file or files such audit trails.	Yes
C1-6	Audit Trail	The system must be able to produce printouts of such audit trails.	Yes
C1-7	Audit Trail	The audit trail must record changes to user access levels and privileges.	Yes
C1-8	Audit Trail	All audit trail entries must be computer generated with the date, local time (hr, min, sec), and operator name. That operator name must be the name of the person carrying out the transaction.	Yes
C1-9	Audit Trail	Where required by predicate rule or business, the system must provide the ability to log the “reason for the change” as part of the audit trail for designated actions/activities on the system.	Yes, reason for change can be added as a Note or Statement
C1-10	Audit Trail	Please confirm the note can be seen in the audit trail.	We have the option to add a Note (no signature required, but author, date and time of the Note is recorded in the audit trail) or a Statement (requiring a signature) that can indicate any changes, modifications or any other events that the user or supervisor wishes to record. These are visible in the audit trail.
C1-11	Audit Trail	The audit trail must keep all entries for original, modified and deleted records.	Yes for original and modified records. Deleted records will also delete the audit trail and we therefore recommend against record deletion. If the user deletes a part of the data file, the audit trail will capture that deletion. However, if the whole data file is deleted the audit trail will also get deleted
C1-12	Audit Trail	Can you block the option to delete records?	There is no “option” to delete records. The data files (and associated audit trails) should be autosaved to a secure location. Security of these files is the responsibility of the system (see URS-SE.12)
C1-13	Audit Trail	All audit trail entries must be linked to the associated electronic record.	Yes
C1-14	Audit Trail	The users must be unable to disable the audit trail.	Yes
C1-15	Audit Trail	The users must be unable to alter the audit trail.	Yes
C1-16	Backup	The system must be able to backup application software and records to alternate media.	Yes, manual backup is possible.
C1-17	Backup	The system must be able to load backup application software and records back into the system	Yes
C1-18	Backup	The system must be able to notify the system administrator of backup results.	No
C1-19	Data Integrity	The system must save automatically all acquired data to a pre-defined destination	Yes
C1-20	Data Integrity	The operator should not be able to modify the destination of electronic records	Yes
C1-21	Data Integrity	The system must keep the date format consistence for all electronic records, reports, logs and audit	Yes
C1-22	Data Integrity	The system must protect electronic record from corruption and falsification	Yes
C1-23	Data Integrity	The system must use auto login in to the operating system when operating system generic user is in use	There is no generic user option, only defined user with password.
C1-24	Data Integrity	The use of generic user in the application is not allowed for the system operators	Yes
C1-25	Data Integrity	The system must ensure that only the system administrator can add, delete or modify users	Yes
C1-26	Data Integrity	The system must limit the number of failed login attempts	Yes
C1-27	Electronic Records	The system shall reject invalid data entries (Ex: character values in number fields, out of range values, etc.).	Yes
C1-28	Electronic Records	The system must be able to produce visual displays of electronic record data and metadata.	Human readable audit trails are produced.
C1-29	Electronic Records	The system must be able to output electronically, to a file or files, electronic record data and their associated metadata.	Yes
C1-30	Electronic Records	The system must check that data input or operational instructions are transferred to/from authorized devices. (terminal, instruments, etc.)	Yes
C1-31	Electronic Records	The system must obtain the date and time used for date/time stamps only from an authorized source that is not modifiable by the user.	Yes, date and time is from the computer operating system.
C1-32	Electronic Records	The system must support the sequencing of operations or events to ensure that steps are followed in the correct sequence across multiple date and time zones.	Unknown – We would need to test that
C1-33	Electronic Records	The system must be able to produce printouts of electronic record data and metadata.	Yes
C1-34	Electronic Records	Printouts created through the system and signed manually shall include a univocal link to the relevant Electronic Record	Yes because the complete Audit trail can be printed. The audit trail shows the file path where the electronic record has been saved
C1-35	Electronic Signatures	The system must check for sufficient authority levels before allowing a record to be signed electronically.	Yes
C1-36	Electronic Signatures	Electronic signatures must contain information associated with the signing that indicates the printed full name, date and time of the signing and meaning (review, approve, author) of the signature.	Yes, except that SMP GxP does not define meaning of signature. Users can add "reviewed" or "approved" to the signature
C1-37	Electronic Signatures	Date and time stamps associated with the electronic signature must be outside of the control of the person signing.	Yes, unless person signing can access the system date and time app.

C1-38	Electronic Signatures	The system must require that no two individuals have the same electronic signature account.	Yes
C1-39	Electronic Signatures	The system must assure that only the user is able to know the electronic signature combination. The system should not display the password during password entry.	Yes
C1-40	Electronic Signatures	The system must be capable of issuing notifications to a designated person of any attempts at unauthorized use of electronic signatures.	System does not issue notifications.
C1-41	Electronic Signatures	Does it show up in the audit trail?	If a user tries to sign and uses the wrong password, and gives up, the audit trail indicates “attempt to sign statement” and “signer failed to verify password”. A failed attempt followed by success is not recorded.
C1-42	Electronic Signatures	Do you block the user that failed to sign as a mitigation ?	No
C1-43	Electronic Signatures	The system must assure that non-biometric electronic signatures consist of at least two distinct components such as an identification code and password.	Yes
C1-44	Electronic Signatures	The system must enforce the use of all signature components during the first signing event.	No
C1-45	Electronic Signatures	Please clarify, do you need to enter user name and password when signing ?	In order to be an active user, you must have already successfully used the user name and password. For signing statements as part of a current session, you need only verify the password for the active user.
C1-46	Electronic Signatures	The system must enforce the use of at least one signature component, known only to the user, for electronic signatures after the first signing event in a continuous session.	The system requires the password but not the user name for the current user in a continuous session.
C1-47	Electronic Signatures	If the electronic signature occurs during a non-continuous session, the system must treat the signature event as a first signing event.	The process is as follows: in a non-continuous session, the user will sign in to the software with username and password. The statement or statements will be created or opened, and a signature added. This signature requires only the password associated with the active user. It is not possible to access signature events without first logging into the software with username and password.
C1-48	Electronic Signatures	The system must require that unauthorized use of an electronic signature require the collaboration of at least two individuals.	No unauthorized signature is allowed.
C1-49	Electronic Signatures	The signature should be permanently linked to the associated record.	Yes
C1-50	Electronic Signatures	The system must require that any biometric signatures, if used, be based upon measuring physical feature(s) or repeatable action(s) that are unique to the individual and measurable.	Biometric signatures are not implemented.
C1-51	Electronic Signatures	The system must assure that the user is the only one who knows the access code corresponding to the user’s unique biometric signature	System does not display passwords and biometric signatures are not allowed.
C1-52	Security	The system must restrict logical access to the system to authorized individuals.	Yes
C1-53	Security	The system must provide multiple user access levels and assign user rights and privileges based upon the assigned job function.	Yes
C1-54	Security	The system must require that no two individuals have the same user access account.	Yes
C1-55	Security	The system must assure that the user is the only one who knows the combination of ID code and Password.	Yes
C1-56	Security	Do you support to force the user to change his password after admin password reset or after user creation ?	Yes
C1-57	Security	The system must enforce password aging and allow a definable period.	Yes, defined as an integral number of months
C1-58	Security	The system must de-activate any account not used for a period specified.	No
C1-59	Security	The system must have the capability to enforce a minimum password length - specified (i.e. 7 characters) or higher.	Yes, minimum 6 characters, at least 1 numeric and 1 alphabetic
C1-60	Security	Is it configurable? E.g. min' 8 characters	No, Password complexity is not configurable.
C1-61	Security	If the system is an "open system" the system must use digital signatures, encryption or other available means when transferring records to ensure record authenticity, integrity, and confidentiality from point of record creation to record receipt.	SoftMax Pro is not an open system and it has an audit trail.
C1-62	Security	The system must have a configurable feature that closes the session after a 15 min of inactivity or a different period specified. (e.g.: Screen Saver or auto log-off). This feature must not be modifiable by users.	Yes
C1-63	Security	If tokens are used, the system must require that tokens or cards bearing or generating user ID or password information have at least one component known only to the user.	Tokens not used
C1-64	Security	The system must prevent a user ID from being reused.	Reuse is not possible.
C1-65	Security	Can you create multiple users with the same user ID ?	No, an active user ID cannot be reused, the system shows an error message when this is attempted. All user IDs must be unique. Also, my error originally – a user ID from a user account that is deactivated cannot be reused.
C1-66	Security	The system must assure that user access to data files can only be done through the system's logical security structure.	Yes, but also requires that Windows permissions be used to restrict access to Windows files and folders. The data files must be saved in a folder or file structure that is not available to the users, to prevent any attempts to modify or delete data. We recommend that Windows permissions are used to prevent unauthorized access of the data files.
C1-67	Security	The system shall require the user to change the password immediately after logging in after the password is reset or created by a system administrator.	Yes

C1-68	Security	The system must notify the system administrator of any attempt of unauthorized use of user access account and provide controls for transaction safeguarding.	No
C1-69	Security	Does it show up in the audit trail?	An audit trail is only created when a data file is saved (we recommend using the autosave function within the software to ensure no unrecorded assays are run). A failure to log in to the software will not create a data file and hence no audit trail.
C1-70	Security	Do you block the user that failed to sign as a mitigation ?	A user can be optionally blocked after 3 consecutive logon failures
C2-1	ER/ES	The system must be able to detect invalid records (such as invalid fields left blank that should contain data, values outside of limits, incorrect file formats, special characters as apostrophe etc.) showing an error message.	It is the responsibility of the customer to set up conditional statements to alert user that the field is blank or invalid.
C2-2	ER/ES	The system must be able to configure the criticality of predefined records such as: Alarms, Automation parameters, Actions	There are no alarms or automation parameters within the system
C2-3	ER/ES	Temporal reference shall be equal for all users and time reference zone has to be clear. Temporal reference cannot be changed by the user	Time zone is based on computer clock and not displayed along with the temporal reference.
C2-4	ER/ES	The system shall allow usage of electronic signatures.	Yes
C2-5	ER/ES	Electronic signatures shall be composed of unique user ID code and a password.	Yes
C2-6	ER/ES	The system must check the authentication and rights of each individual e-signing a record via Domain Controller (if possible)	Authentication and rights are checked by reference to the .edb database defined by the GxP Admin software. GxP Admin may be functionally equivalent to Domain Controller
C2-7	ER/ES	The system shall allow configuring the operations to be performed by means of electronic signature and the user groups that have the right to perform it.	Yes.
C2-8	ER/ES	The system must allow choosing between single, double or no signature when an input (data entered by user) is inserted.	Number of signatures can be configured.
C2-9	ER/ES	If a double signature is required, the system must enforce the signers are two different users with appropriate authorization	There is no enforcement, only the opportunity for different users.
C2-10	ER/ES	Signed electronic records must contain information associated with the signing that indicates all of the following: The printed name of the signer, the date and the time the signature was executed, the meaning associated with the signature (e.g., review, approval, responsibility, or authorship) or the reason, manually entered. The information above, associated with the signing, must be included as part of any human readable form of the electronic record (such as electronic display or printout).	Printed name, date, time and a note can be added. Signatures and associated text form part of the audit trail.
C2-11	Audit Trail and / or Version control records	The system must be able to generate audit trail for configured records. Audit trail record must contain: 1. User who performed the action, 2. Date and time stamps of the action (time zone reference has to be clear), 3. The entry/value prior to the change 4. The entry/value change, 5. The reason for the change (this would not be automatically generated, but manually entered by the user) when records are modified.	1. Yes, 2. Yes (there is no time zone reference), 3. Yes, older data is not deleted from audit trail., 4. Results are also recorded, 5. Yes, Notes and Statements can be added when records
C2-12	Audit Trail and / or Version control records	The changes executed on the following records must be under audit trail: 1. User Log in, 2. Failed log in, 3. User creation, 4. Changes to the user accounts, 5. Password changes, 6. Changes to user profiles privileges, 7. Critical alarms acknowledge, 8. Critical command enabling / disabling, 9. Critical parameter, 10. Start/Stop process	1. Yes, 2. No, 3. Yes within GxP Admin audit trail, 4. Yes within GxP Admin audit trail, 5. Yes within GxP Admin audit trail, 6. Yes within GxP Admin audit trail, 7. NA, 8. NA, 9. NA. 10. Yes
C2-13	Audit Trail and / or Version control records	The system shall allow retaining the generated audit trails at least as long as the records to which they pertain.	Yes
C2-14	Audit Trail and / or Version control records	The system must not allow Audit Trails configuration, modification or deactivation at not administrative roles.	Yes
C2-15	Audit Trail and / or Version control records	The system must not allow users to change any data automatically captured without audit trail.	Yes, but Windows permissions must also be used to prevent users gaining access to data files.
C2-16	Audit Trail and / or Version control records	The system must be able to create version controlled records. The changes executed on the following records must be under version control. Typically, version controlled records must be (as applicable) recipes (e.g. automation, production)	Version control is not implemented but different versions can be created by changing the file name.
C2-17	Audit Trail and / or Version control records	The system must be able to configure the approval signatures of the version control records. Typical creation and approval levels are: Writer, Reviewer, Approver	SMP GxP does not define signature levels but differnent statements can be inserted. When the statements are signed the name of the signer is added.
C2-18	Audit Trail and / or Version control records	The system must be able to show the comparison result of the sequential versions of a recipe	A comparison receipt can not be displayed
C2-19	Audit Trail and / or Version control records	The system must be able to set as effective and use only the last approved version controlled records	This must be configured by authorised controller by using folders with access permissions.
C2-20	Logical security & Access Limitation	The system must be able to permit a unique user ID and password for logging in a user via Domain Controller System (if possible)	System allows unique user id and password login, controlled via GxP Admin.
C2-21	Logical security & Access Limitation	The system must not permit the display or printing of passwords when they are entered into the system.	Yes
C2-22	Logical security & Access Limitation	The system must allow only authorized users to create, change, deactivate/re-activate user accounts	Yes via GxP Admin software
C2-23	Logical security & Access Limitation	The system must allow the configuration of multiple access levels to allow segregation of duties. Typical HMI access levels are: Read only, User, Power user, Maintenance, Administrator	Roles and permmissions can be freely configured via GxP Admin software.

C2-24	Logical security & Access Limitation	The system must allow the configuration of access rights to the different access levels. Typical access rights are:, NA (Read only), Start and stop functionalities, Acknowledge alarms (User) , Double signature authorization step, (Power user), Troubleshooting (Maintenance), Security management, problem solving, configuration changes (Administrator)	Configuration is set via GxP Admin by authorised user. If all specif requirements can be fullfilled have to be tested in a demo.
C2-25	Logical security & Access Limitation	The System must include an automatic log off mechanism after a pre-defined period of user inactivity, or a mechanism where user ID entry is required after inactivity period.	Yes, set in GxP Admin software
C2-26	Logical security & Access Limitation	The system must have a logout functionality to be activated by the user.	Yes in SMP GxP
C2-27	Logical security & Access Limitation	The system must be able to force passwords to expire after a configurable number of days via Domain Controller System (if possible)	Password aging defined by integral number of months
C2-28	Logical security & Access Limitation	The system must automatically prompt the users to change their passwords upon first entry and upon expiration via Domain Controller System (if possible)	Yes to both requirements
C2-29	Logical security & Access Limitation	The system must not allow users to reuse the last N password where N is a configurable number via Domain Controller System (if possible)	No
C2-30	Logical security & Access Limitation	The system must control the password length and shall require special character in password via Domain Controller System (if possible)	Password must be at least 6 characters and contain at least 1 numeric and 1 alphbetical character.
C2-31	Logical security & Access Limitation	The system must display an error message if an invalid user id is entered via Domain Controller System (if possible)	Yes via SMP GxP interface
C2-32	Logical security & Access Limitation	The system must display an error message if the user enters an incorrect password via Domain Controller System (if possible)	Yes via SMP GxP interface
C2-33	Logical security & Access Limitation	The system must lock the user account after an established number of authentication failures via Domain Controller System (if possible)	Yes, 3 attempts allowed
C2-34	Logical security & Access Limitation	The system must only allow authorized users to unlock a user account as a consequence of a definable number of failed login attempts via Domain Controller System (if possible)	Yes via GxP Admin
C2-35	Logical security & Access Limitation	The system must lock the user account after a configurable number of unsuccessful attempts to provide the correct password when executing an electronic signature via Domain Controller System (if possible)	User account is locked after 3 failed log-on attempts
C2-36	Logical security & Access Limitation	Upon initialization and after a logout, the system must start to the unit default view screen	Yes
C2-37	Logical security & Access Limitation	System time and date must be synchronized with Windows Domain Server.	If the client computer is synchronised then system time at date will be.
C2-38	Logical security & Access Limitation	The system shall not allow users, except for administrator, to access the operating system or configuration files and any data stored on file outside of the application (e.g. via lock down software).	This will depend on Windows permissions settings.
C2-39	FUNCTIONAL	In case a modification of critical parameter or in case an enable/disable of critical functionality is allowed on Machine HMI, it must be temporary (limited to that lot). The system must be able to automatically reset parameters changes or command enabling / disabling, in a pre-defined phase of the process (e.g. at equipment set up the control system must restore the original parameters based on the current machine recipe)	Reversion to previous settings will occur unless changes are saved.
C2-40	FUNCTIONAL	The system must allow the parameter modification only if the new value is within the predefined limits.	Yes
C2-41	FUNCTIONAL	The system shall have operational checks in order to enforce permitted sequencing of steps and events by allowing the execution of one step only after the execution of the previous one (Apply only if particularly critical operations are performed through the System). E.g. critical alarms must be reset only if the alarm condition has returned to normal condition and an authorized user has acknowledged the alarm.	NA
C2-42	FUNCTIONAL	If the system is interfaced with other system or equipment, it must be able to identify the validity of the source data.	NA
C2-43	FUNCTIONAL	The system must be able to define configurable parameters (tags, recipe names, WorkCentre units) to interface with an external system	NA
C2-44	FUNCTIONAL	The system must be able to generate the appropriate machine reaction (error message, alarms, stop the process) in case of data transfer failure.	YES
C2-45	FUNCTIONAL	The system must be able to periodically monitor the data transfer functionality is up and running	Test measurements via validation plates
C2-46	FUNCTIONAL	If there is a system interface, the system must be able to resynchronize successfully after start-up, including the ability to detect any data that was not properly sent/received.	No
C2-47	FUNCTIONAL	The system must allow Process parameters values to be archived in the data historian at appropriate intervals.	NA
C2-48	FUNCTIONAL	The system must allow retaining the configuration and generated data for all the record retention period	Storing and archiving data has to be fullfilled by the IT department.
C2-49	FUNCTIONAL	The system must allow retaining the generated audit trails at least as long as the records to which they pertain.	Yes
C2-50	FUNCTIONAL	The system must be able to store Data temporary buffered in local DB (e.g. SQL) in appropriate DBs for the required retention period. For temporary buffer the storage time interval and buffering cleaning process must be defined. Overflow of buffering must be alarmed.	Filepath can be specified across network. There is no buffering or local database
C2-51	FUNCTIONAL	The system shall automatically and contemporaneously save all electronic records created by user or by the system itself (in a secure database as preferred or in a secure directory), alternatively must force the user to save it.	Yes
C2-52	FUNCTIONAL	When a manual saving is required, the system shall not allow to save a record over another record without audit trail and shall warn the user showing an error message	Yes

C2-53	FUNCTIONAL	The system must allow the periodic change of the System accounts passwords	Yes
C2-54	FUNCTIONAL (Reporting)	The system must be able to provide a report with the details of a specific audit trailed record e.g.: 1. Login attempts, 2. User privileges, 3. Family group privileges	1. Yes, 2. Yes, 3. Yes
C2-55	FUNCTIONAL (Reporting)	The system must be able to provide dedicated report of each process cycle in scope	Yes
C2-56	FUNCTIONAL (Reporting)	The System must allow to generate accurate and complete copies of electronic record in both human readable (e.g., screen display or printouts) and electronic format suitable for inspection, review and copying. If it is technically feasible, it should be provided to a regulatory agency the ability to search, sort, or trend records always preserving the content and the meaning of the record. Electronic records reports must include (as applicable):, 1. Audit trails (e.g. Login attempts, parameters/actions), 2. Process cycles, 3. Automation recipe data, Alarms. 4. In process control data	1. Yes, 2. NA, 3. NA, 4. NA
C2-57	FUNCTIONAL (Reporting)	The system must be able to provide a report with the details of a specific version controlled object including the SQL Statements and the signature data.	Full reports are possible but we do not use an SQL based system
C2-58	FUNCTIONAL (Reporting)	The system shall not allow end user to change the content of report including or excluding any of the data from the report. As alternative the audit trail of change of the content must be tracked.	Yes