Adroit Smart SCADA 21 CFR 11 mode

21 CFR Part 11 (21 CFR 11) of the Code of US Federal Regulations is a standard that defines the criteria and circumstances under which electronic records are considered to be trustworthy, reliable and equivalent to paper records by the United States Food and Drug Administration (FDA). This includes the auditing and authorization of changes to values.

It deals with FDA guidelines on electronic records and electronic signatures (ERES). These define the criteria and circumstances under which ERES are considered to be trustworthy, reliable and equivalent to paper records by the FDA. In short, those records that remain subject to part 11, need to adhere to the following requirements:

- validation of computerized systems
- generation of time-stamped audit trails to ensure the trustworthiness and reliability of the records
- provision to investigators of reasonable and useful access to records during an inspection

21 CFR 11 also requires that the following controls and requirements be implemented:

- limiting system access to authorized individuals
- use of operational system checks
- use of authority checks
- use of device checks
- persons who develop, maintain, or use electronic systems have the education, training, and experience to perform their assigned tasks
- establishment of and adherence to written policies that hold individuals accountable for actions initiated under their electronic signatures
- appropriate controls over systems documentation

During initial engineering, a system is not required to comply with 21 CFR 11. It is only once the system is deployed that compliance may be required.

Therefore, you should ideally engineer your project, with 21 CFR 11 mode disabled, due to the design-restrictions that it imposes and then just before commissioning you can enable 21 CFR 11 mode. For more details of the controls and requirements see 21 CFR 11 controls and requirements in the Adroit Smart SCADA help pages.

Note: 21 CFR 11 mode is enabled in the Server Security Settings page of the Adroit Config Editor utility.

What 21 CFR 11 mode enforces

21 CFR 11 compliance requires limiting system access to authorized individuals. Therefore the connection to the server components must be secured in order to limit exactly which client connections are allowed. This prevents unsanctioned access (including Classic UI Clients and third party applications).
Note: This means that you cannot use the Classic UI Configurator when using 21 CFR 11 mode - so all server configuration must occur from the Designer application

ADROIT
TECHNOLOGIES
Tel: +44 1270 627 072
Adroit Technologies Ltd
PO Box 19 Nantwich
Cheshire England CW5 6FF
www.adroit-europe.com

directly. Changing a data element value may only be allowed when an additional user provides authorization that this change in value can be made.
Note: Any change that does not received authorization is not carried out and is purged if authorization is denied. All changes to data element values must be recorded with the user who initiated the change and if applicable the user who authorized this change. These logged changes include: the timestamp of the change; the change made; the initiating user; if applicable the authorizing user; a computed hash value of all these fields to detect possible tampering. For this reason the server components include data element security features, as follows:

- **auditing:** to audit ANY data element by completely tracking changes made to its value via the Operator UI
- **change authorization:** when enabled this requires an additional user to provide authorization before a change can be made to a data element

This functionality forms a core component in the server components and is underpinned by a database

Configuration Requirements

First, the required users and/or groups need to be created within Windows. Each of these users and/or groups need to be configured as "allowed" users and groups on each server, before they are able to log in and/or audit and/or authorize changes made to data element values.

If users are required to access the server computer(s) directly then to preserve the integrity of the 21 CFR 11 functionality, these users must only be given minimal rights (from a Windows security context). Only administrative users may be given extended rights.

IMPORTANT: Therefore ONLY specify your system administrator users and/or groups in this the **Security Settings** page for the Smart UI Server in the Adroit Config Editor, since these users and/or groups will have immediate GLOBAL access to every aspect of the project, which includes the ability to write to all of the data elements.

The configuration (.config) files on the server computer(s) must be made inaccessible (through directory and file level security) to prevent unauthorized users from:

- disabling the 21 CFR 11 setting thereby “turning off” the audit mechanism entirely and the use of the secure connection to the Adroit Agent Server
- deleting the mandatory local secure SQL Server Compact database that stores the 21 CFR 11 auditing

If you choose to use a separate SQL Server database to store the 21 CFR 11 auditing then you will need to prevent unauthorized users from accessing this database too.