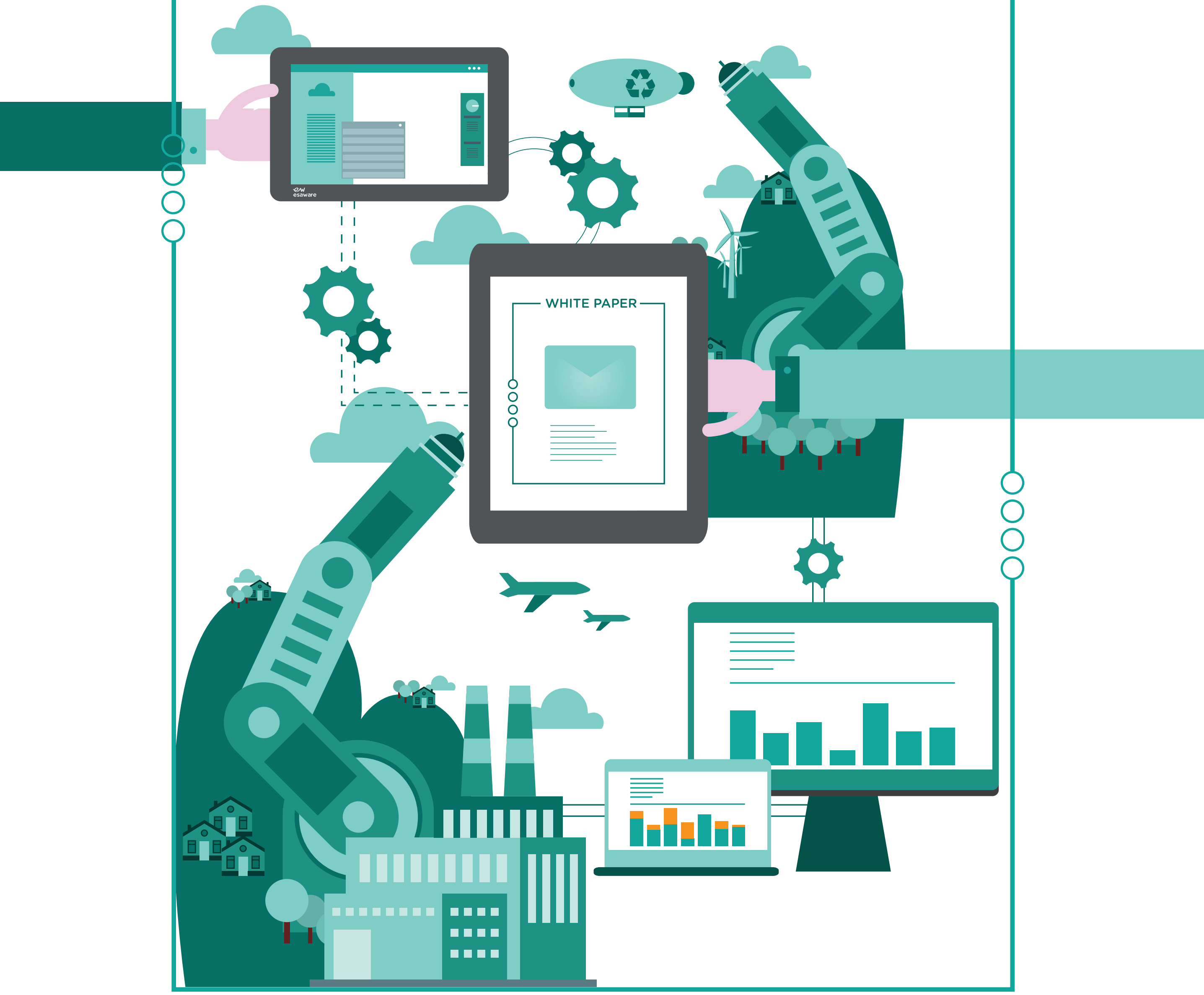
n.1

year 2016

ESA AUTOMATION
Connect ideas. Shape solutions.

WHITE PAPER

The Heart of Automation and the Art of Innovation



www.esa-automation.com

What is the FDA?

The FDA (Food and Drug Administration) is the American agency responsible or the control and regulation of production processes in the food, pharmaceutical and chemical sectors.

In other words, it makes sure that all requirements rules and standard are met in these areas.

To be under its authority are not only US firms, but all companies that operate and export in the United States. Including ESA Automation.

What is the 21 CFR Part 11?

The 21 CFR is a regulation emanated by the FDA in 1997 in collaboration with the USA government, that regards the use of technology in some procedures of the production process.
Specifically, Part 11 is divided into two main sections:

- Electronic Records
- Electronic Signatures

Therefore, the 21 CFR Part 11 regulates the way we manage data that are saved on an electronic support and the related safety measures.

Why is the 21 CFR Part 11 so important?

The aim of the 21 CFR Part 11 is to allow the broadest and safest usage of technology in the industrial field. In order for this to be possible, it is necessary to verify that all the procedures of the production process comply with certain requirements.

What are the most important requirements of the FDA 21 CFR Part 11?

The 21 CFR Part 11 sets four fundamental points to be observed.

- The need to have a centralized system for managing accounts, including the obligation of access through login with a username and a password.
- Automatic separation of roles (administrator, technical analyst, operator, etc.).
- The presence of a standardized reporting system in order to generate accurate and complete copies of records that can be read electronically.
- The traceability of each individual operation, which must be part of a historic consultation at any time in the form of standard reports.

	Compliance points	Yes (√) / No (×)
Instrument/Equipment and Software shall have facility to :		
1.	**Password policy**	
1.1.	Password-protected individual user accounts.	YES
1.2.	Password and User ID policy (Individual unique ID and Password, minimum length and strength of ID and Password).	YES
1.3.	After generation of user ID (user creation) system shall ask for password change on first login.	YES
1.4.	Automatically limit number of failed login attempts.	YES
1.5.	Automatically record unauthorized login attempts.	YES
1.6.	Electronically require users to change their passwords at regular intervals.	YES
1.7.	System shall ask to change the password to user periodically (at settable interval of time) by giving prior notification on each logging. Time for prior notification shall be setable at user end.	YES
1.8.	Automatically password protects computer/ SCADA systems when idle for short periods.	YES
2.	**User management system & Privileges**	
2.1.	Ensure that the user level based on functionality and authority is defined.	YES
2.2.	Facility to create the groups such as operator, supervisor, manager, administrator, maintenance, calibration etc and allocation of their user privileges can be define and can be changed as per requirement at site.	YES
2.3.	Ensure that the privileges like delete, copy, cut, paste, rename, etc. shall not be allowed to un authorized user.	YES
3.	**Electronic Data**	
3.1.	Electronic data and report should be human readable and suitable for inspection and review.	YES
3.2.	Ensure the content: Performed by with date and time stamp, Print by with date and time, Reviewed by with date and time stamp, system and analysis parameter related information, etc.	YES
4.	**Electronic data storage.**	
4.1.	Only authorized users can access configuration screen and partitions of hard disk.	YES
4.2.	Generated data shall not be edited or altered.	YES
4.3.	Data should be saved automatically to pre define location.	YES
5.	**Audit Trail**	
5.1.	System should track for all creations, modifications, and deletions performed in the system (All activity should be logged between login and log out) with time and date stamp along with user details.	YES
5.2.	All critical hardware related errors and warning should be logged in audit trail (System audit trail).	NO
5.3.	Maintain all entered data: Don't obscure original data when changes are made (shall maintain revision history for the changes made).	YES

5.4.	Time and date stamp change automatically, it shall be locked and not editable unless performed by authorized user (shall be defined through user rights distribution).	YES
5.5.	Computer/SCADA system shall be designed in a way that user to record reason for change through use of authorized login / password to go ahead with changes.	YES
5.6.	Automatically record identity of individual who made change.	YES
5.7.	System shall prevent to modify or delete audit trail.	YES
5.8.	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 if required. At least for 5 years.	YES
6.	**User management system & Privileges**	
6.1.	**Electronically signature documents have following content (Automatically generate)**	
6.1.1.	The printed name of the signer.	YES
6.1.2.	The date and time when the signature was executed.	YES
6.1.3.	The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	YES
6.1.4.	The items identified in paragraphs 6.1.1, 6.1.2, and 6.1.3 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)."	YES
6.2.	The unique ID and Password for electronic signature.	YES
6.3.	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.	YES
6.4.	The each process of electronic signature should be electronically logged in audit trail with time, date stamp and user ID.	YES
6.5.	Uniqueness to be maintained between password and ID, Both are same is not acceptable by system.	YES
7.	**Data Backup.**	
7.1.	Software shall have facility for auto data back-up to any client or connected central server.	YES
8.	**Other**	
8.1.	User shall not be able to save or relocate the result files, it should be controlled through software only.	YES
8.2.	User shall not have rights to create folders or project in software, these rights shall be with administrator.	YES

ESA elettronica S.p.A.
Via Padre Masciadri 4/a
22066 Mariano Comense (CO) -Italia
Tel. +39 031 757400
Fax. +39 031 751777

ESA elettronica S.p.A.
Unità locale di Bentivoglio
Via Monari Sardè 3
40010 Bentivoglio (BO) Italy
Tel. +39-051-6640464
Fax +39-051-6640784

ESA Europa S.L.U.
Passeig del Ferrocarril, 335
08860 Castelldefels (Barcelona) - España
Tel. +34 936455014
Fax. +34 936455013

意萨电子科技（上海）有限公司
中国上海市宜山路889号齐来工业城4号楼6层D1
ESA Electronic Technology (Shanghai) Co. Ltd
Unit D1, 6F, Bldg. 4#, No. 889 Yishan Road
Shanghai 200233 - P.R.China
Tel. +86 21 6090 7250
Fax +86 21 6090 7258

ESA Technology Inc.
780 NW York Drive Suite 202
Bend, OR 97703 U.S.A.
Tel. +1 707 5447300
Fax. +1 541 7492208

ESA energy S.r.l.
Via Fortunato Zeni 8
38068 Rovereto (TN) - Italia
Tel. +39 0464 443272
Fax. +39 0464 443273

ESA elettronica S.p.A.
Unità locale di Pontedera
Via Molise,1 - Z.I. Gello
56025 Pontedera (PI) - ITALY
Tel. +39 0587 296014
Fax. +39 0587 294240

ESA Elettronica GmbH
Carl-Zeiss-Str. 35
D-63322 Rödermark
Tel : +49 6074 486 45 22
Fax: +49 6074 486 45 66

ESA Software & Automation India Pvt. Ltd
Ist Floor, 2nd Main,HRBR Layout,
3 rd Block,Kalyan Nagar Post,
Bangalore 560 043 - India
Tel. +91 80 25435656

ESAElektronik Technology Ticaret Limited Şirketi
Şerifali Mah., Çetin Cad. Kıble Sk.
No: 6 Of Plaza Kat: 5 D.: 7
Ümraniye/İstanbul - Türkiye
Tel. +90 216 466 70 33
Fax. +90 216 466 70 99

www.esa-automation.com