YOKOGAWA

CENTUM CS3000 R3

Achieving 21 CFR Part 11 Compliance using CENTUM CS 3000 R3

Authored by:

stelex

Table Of Contents

1 ABSTRACT 3

2 21 CFR PART 11 GENERAL REQUIREMENTS.....3

2.1 WHY ELECTRONIC RECORDS & ELECTRONIC SIGNATURES.....4
2.2 YOKOGAWA'S COMMITMENT.....4

3 DEFINITIONS, ABBREVIATIONS, AND ACRONYMS 6

4 CS 3000 DESCRIPTION 8

4.1 WHERE USED 8
4.2 CONFORMS TO INDUSTRY STANDARDS.....8
4.3 SCALABLE & READY TO INTEGRATE 9
4.4 SYSTEM CONCEPT AND CONFIGURATION 9
4.4.1 HMI Stations.....10
4.4.2 Field Control Station (FCS) 11
4.4.3 Communication.....11
4.4.4 Access Control Utility.....12
4.4.5 Electronic Records.....13
4.4.6 Electronic Signature.....15
4.4.7 Report package 15

5 CENTUM CS 3000 - DETAILED PART 11 COMPLIANCE.....16

5.1 GENERAL PROVISIONS (SUBPART A).....17
§11.1 Scope.....17
§11.2 Implementation.....17
§11.3 Definitions 18
5.2 ELECTRONIC RECORDS (SUBPART B) 20
§ 11.10 Controls for closed systems. 20
§ 11.30 Controls for open systems.....27
§ 11.50 Signature Manifestations 28
§ 11.70 Signature/record linking.....29
5.3 ELECTRONIC SIGNATURES (SUBPART C) 30
§ 11.100 General requirements.....30
§ 11.200 Electronic signature components and controls.....32
§ 11.300 Controls for identification codes/passwords 34

1 ABSTRACT

This technical white paper will discuss Yokogawa's CENTUM CS 3000 R3 DCS (Distributed Control System) product, hereafter referred to as "CS 3000", and the extent of its compliance with Part 11 of Title 21 of the Code of Federal Regulations, (21 CFR Part 11), the Electronic Records / Electronic Signatures Rule.

CS Batch 3000 is the optional Batch control package for CS 3000, which provides recipe management and process management functionality based upon the ISA-88 Batch Control System standard.. This whitepaper addresses the use of CS 3000 and CS Batch 3000.

A detailed analysis of Part 11 was performed, the results of which are listed in the Detailed Part 11 Compliance section (section 5) of this document, which supports the compliance of the CS 3000 system to Part 11.

CS 3000 is a comprehensive software package containing configurable functions that support Part 11 compliance (audit trails, electronic signatures and electronic records). The system capitalizes on its Part 11 compliance attributes in the marketing strategy of supplying FDA regulated industries with state of the art automation capabilities.

User training and education as well as the development and utilization of policies and procedures are key components of Part 11 compliance which must be established by the user.

2 21 CFR PART 11 GENERAL REQUIREMENTS

Part 11, a regulation issued by the Food and Drug Administration (FDA) in August, 1997 , provides criteria for the acceptance of electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper.

Part 11 applies to any records required by FDA statute or regulations which are kept electronically, such as batch records. Computer systems subject to Part 11 must be validated, this requirement satisfied by employing the SDLC (System Development Life Cycle) methodology utilized by most companies.

Part 11 establishes that there must be reliability in the integrity of records being generated by a computer system and stored electronically. Additionally, these electronic records must be available in human readable and electronic forms that are both accurate and complete, and suitable for inspection, review and copying by the FDA. It further stipulates that only authorized personnel may have access to these systems and that audit trails are in place to ensure that assure these systems, and their records, are operated and maintained properly. That is, computer systems must be operated and maintained by authorized and qualified individuals possessing applicable training and/ or experience.

Not all requirements of the Part 11 regulation can be addressed solely by the computer system, as with the aforementioned user qualifications. Standard Operating Procedures (SOPs) must be developed, implemented and maintained to ensure that these requirements are addressed. Procedures must be also be developed to govern the maintenance of the Part 11 compliant computer systems as well as system administration and access. .

Training programs need to be implemented and maintained to accommodate possible system upgrades and changing business models to further guarantee the qualifications of individuals who operate the systems. The determination that persons who develop, maintain, or use electronic record/ electronic signature systems have the education, training and experience to perform their assigned tasks cannot be automated.

2.1 Why Electronic Records & Electronic Signatures

The benefits of electronic record keeping, executed in accordance with Part 11, are reduced costs and increased efficiency. This is achieved by simplifying storage associated with the elimination of paper document storage, provide data / integration trending capability leading to improved process control, and increasing the speed of information exchange and accessibility.

With the original predicate regulations (GLPs, GMPs, GCPs) written/interpreted in the late 1970s and early 1980s, the general aim of the Part 11 regulation, was to address the change from a paper based environment to an electronic based environment. The regulation was to provide the opportunity to utilize electronic records while still being compliant with the predicate regulations.

The configurable, ‘off the shelf’ computer systems reduce the efforts necessary for their implementation. The arduous task of performing the evaluation, of whether the system is Part 11 compliant or not, is greatly reduced when the manufacturers of such systems develop their products with Part 11 compliance in mind.

2.2 Yokogawa’s Commitment

Yokogawa has a long and substantial history as a world leader in industrial automation and control, test and measurement, information systems, and industry support. Yokogawa has secured more than 4,500 patents and registrations, representing a number of important innovations, including the world's first DCS (distributed control system) and the first digital sensors for flow and pressure measurement.

Yokogawa contracted Stelex to perform an evaluation of the CS 3000 DCS product with respect to the Part 11 regulation. CS 3000 is a valuable process control and batch tool allowing business benefits to users in continuous or batch processing applications focusing on Key Process Performance Indicators. CS 3000 is designed to support compliance with the Part 11 regulation, thus utilizing the efficiencies and latest technology associated with electronic records and electronic signatures.

Stelex performed the CS 3000 evaluation by assessing the applicability of Part 11 to the application (CS 3000, R3.04.00). Key assumptions made during the evaluation were that the application:

(1) Must comply with all requirements of Part 11; and

(2) Will not be used in open systems as defined in Part 11.

A detailed checklist based on the requirements of Part 11 was developed, and the application assessed for its applicability and level of compliance.

Yokogawa maintains its position as a global leader not only in the manufacture and supply of instrumentation, but in process control and automation solutions as well.

3 DEFINITIONS, ABBREVIATIONS, AND ACRONYMS

Term	Description
Biometrics	A method of verifying an individual's identity based on measurement of the individual's physical features(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable (21 CFR §11.3(b)(3))
CFR	Code of Federal Regulations
cGMP	Current Good Manufacturing Practice
CSV	Comma Separated Values – database export/ import format and file extension
DCS	Distributed Control System
Electronic Record	Any combination of text, graphics, data, audio, pictorial, or other information represented in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system (21 CFR §11.3(b)(6))
Electronic Signature	A computer data compilation of any symbol or series of symbols executed, adopt, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature. (21 CFR §11.3(b)(7))
ENG	Yokogawa Engineering Workstation
ERP	Enterprise Resource Planning
FCS	Field Control Station
FDA	Food and Drug Administration
FIO	Field Input Output – Yokogawa hardware for integrating field I/O with the FCS
GSGW	CS 3000 Generic Subsystem Gateway station used to integrate OPC compliant systems
HIS	Yokogawa Human Interface Station used by system operators to perform system operations and/ or report generation and printing depending on user access rights
HMI	Human Machine Interface
I/O	Input / Output; IO
ID	Identification
ISA-88	Batch control standard, released by the International Society for Measurement and Control (ISA) in 1995, defining models and terminology for batch manufacturing and batch control. Also referred to as S88.

LAN	Local Area Network
LIMS	Laboratory Information Management System
Master Validation Plan	Provides a systematic approach that shall be used to validate a computer system to ensure verification that all validation testing, procedures, and training are completed prior to the manufacture or release of a product.
MES	Manufacturing Execution System
ODBC	Open Data Base Connectivity
OPC	Method of open data exchange between manufacturing system based upon standards by the OPC Foundation
PDA	Personal Digital Assistant
PDF	Portable Document Format (Adobe Acrobat)
PID	Proportional, Integral, Derivative
PIMS	Plant Information Management System, refer to the Exaquantum/Batch Part 11 whitepaper for more information.
PLC	Programmable Logic Controller
PRM	Plant Resource Manager, Yokogawa asset management package
ProSafe	Yokogawa safety system
RDB	Relational Data Base
RIO	Remote Input Output - Yokogawa hardware for connecting Yokogawa RIO
SEBOL	**Se**quence and **B**atch **O**riented **L**anguage, a programming language designed for process control by Yokogawa.
SFC	Sequential Function Chart
SLC	System Life Cycle
SOP	Standard Operating Procedures
Vnet/IP	Yokogawa communication protocol network
XLS	Filename extension for Microsoft Excel spreadsheet file

4 CS 3000 DESCRIPTION

Yokogawa's CS 3000 is an integrated production control system scalable from small to very large process control applications that has been developed with Yokogawa's industry experience and knowledge.
CS 3000 supports basic regulatory (e.g., PID) and sequence control, along with batch control and process management functions based on ISA-88 standards. It can handle multi-product, multi-train high volume production.

The control station/HMI is broken into two components that may exist on the same PC: the Engineering Station (ENG) and the Human Interface Station (HIS). Communication between field components and the HMI is achieved via the Yokogawa Vnet/IP communications network.

4.1 Where Used

CENTUM CS 3000 is widely used in the petroleum refineries, petrochemical, food, chemical, pharmaceutical, paper and pulp, steel and non-ferrous metals, cement, power, gas, water and waste water industries in Europe, Asia, Japan, and the Americas. Yokogawa continues to strengthen its focus on the pharmaceutical industry with emphasis on compliance with Part 11 in all of its software based products.

4.2 Conforms to Industry Standards

In addition to compliance with Part 11, CS 3000 conforms to the following industry standards:

a) CS 3000 is built on the ISA-88 standard thereby possessing the capability of reusing unit definitions and providing complete control capabilities to enterprise level hierarchy of activities (process control, unit supervision, process management, recipe management).
b) Foundation Fieldbus, a bi-directional communications protocol used for communication among field instrumentation and control systems, is also supported by CS 3000.
c) OPC – Object Linking and Embedding for Process Control that provides open connectivity for data exchange between systems and applications

4.3 Scalable & Ready to Integrate

CS 3000's open interfaces facilitates data access from supervisory systems such as Enterprise Resource Planning (ERP) Systems, Manufacturing Execution Systems (MES), and Laboratory Information Systems (LIMS) making it easy to create a strategic management information system for an enterprise. CS 3000 is a scalable, compatible system - designed to work with existing systems, and grow with the users' business, reducing total cost of ownership.

Tag Capacity

CS 3000 supports up to 100,000 tags in its standard configuration and can be expanded to support up to 1,000,000 tags.

Compatible

CS 3000 is backward compatible with the CENTUM family predecessors and can be integrated with other control systems. CENTUM V and CENTUM-XL can be migrated to CS 3000 without changing field devices and wiring to I/O cards in existing FCS (Field Control Station).

Network

CS 3000's Vnet/IP provides a highly reliable control network offering redundancy and deterministic level response using Internet Protocol (IP) on a 1 Giga-bit per second. With Vnet/IP general communication functions co-exist with control functions enabling easier integration of CS 3000 with other systems.

CS 3000 can support up to 256 control and HMI stations distributed over a maximum of 16 domains with up to 64 stations per domain, HIS stations are limited to 16 per domain. Existing Vnet based systems can be connected to Vnet/IP based systems to ease upgrades to CS 3000.

4.4 System Concept and Configuration

The basic components of the CS 3000 system as shown in Figure 1 are:

a) Human Machine Interface (HMI)
   - Engineer Station (ENG)
   - Human Interface Station (HIS)

b) Field Control Station (FCS)
   - Supports a wide set of field buses including Foundation Fieldbus, HART, Modbus, DeviceNet, Ethernet, and Profibus.

c) Plant Resource Manager (PRM) for asset management

d) Generic Subsystem Gateway (GSGW) for integrating OPC servers with CS 3000 Function Blocks

e) Exaopc for OPC Data Access, Alarm & Event, Historical Data Access and Batch servers

f) Exaquantum/Batch, Yokogawa's Batch Plant Information System (PIMS) may be tightly integrated with CS 3000 to collect and store Electronic Batch Records (EBR)

g) Communications

- Vnet/IP is a 1 Giga-bit per second Internet Protocol based network supporting CS 3000 control communications and general purpose Ethernet communications.
- Switches may be added to integrate other Ethernet based control, MES and information systems such as OPC servers and PLCs.

Yokogawa also offers a safety system, Prosafe, which can be integrated with CS 3000.

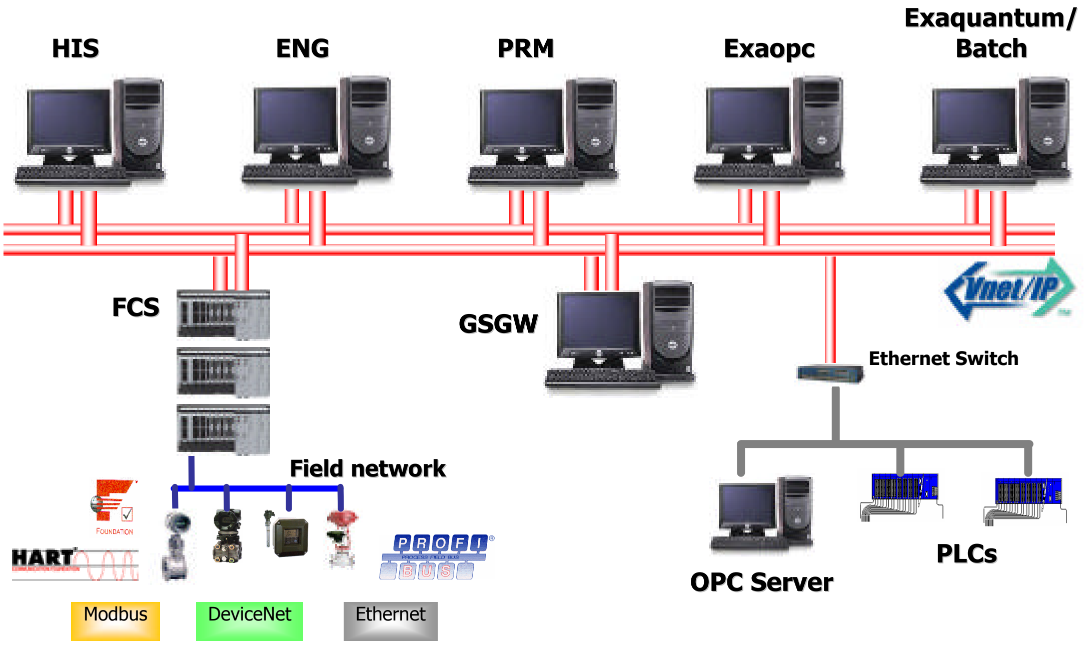


Figure 1 – Typical CS 3000 Configuration

4.4.1 HMI Stations

CS 3000 consists of two types of HMI stations (HIS and ENG) that may exist on the same computer, depending on user requirements. Users can use the CS 3000 System View Test Function (control station emulation) to provide an efficient and easy to use engineering environment for application development and testing. The HIS PC can be mounted in an HMI console or exist in a desktop arrangement.

CS 3000 can be run on PCs with Windows 2000 Pro, Windows 2000 Server, Windows 2003 Server or Windows XP Pro operating systems. Remote operation capabilities permit collaborative engineering during application development, remote operation within a plant and faster response by support personnel during operation.

CS 3000 HIS and ENG stations have these basic functions:

a) Engineering function - process control development via the ENG station (via a combination of Structured Text (SEBOL), Logic Charts and SFC type programming environment)

b) Operator interaction and display via real time plant mimics and displays

c) Alarm and event management, display, storage and retrieval

d) Trend display, storage and retrieval

e) Data archiving, backup and restoration

f) Report generation and printing via HIS stations

g) Recipe management via a separate PC or integrated with the ENG station

4.4.2 Field Control Station (FCS)

Field control stations (FCS) perform real-time control functions in CS 3000. Using function blocks, logic charts, sequence tables and a structured text programming language an FCS can be used to control and monitor a few equipment modules or multiple units.

There are two types of Field Control Station hardware: FCS for FIO (fieldnetwork I/O) and FCS for RIO (remote I/O). There are also standard and compact sized FCSs.

a) FCS for FIO – This uses the compact Yokogawa FIO modules, standard or enhanced modules are utilized based on user capacity requirements.

b) Compact FCS for FIO – This is a compact FCS with I/O modules integrated into the Field Control Unit.

c) FCS for RIO – This FCS uses the Yokogawa RIO modules. Standard or enhanced modules are utilized based on user capacity requirements.

d) Compact FCS for RIO – This controller is usually installed near the equipment or process it controls, and is ideal for communicating with subsystems.

4.4.3 Communication

Communication between the main components is achieved via Yokogawa's Vnet/IP communications network. Vnet/IP is a 1 Gigabit per second network providing real-time control system bus functionality co-existing with general purpose Ethernet communications. Vnet/IP offers secure, highly reliable, redundant, communications using commercially available networking equipment.

With Vnet/IP the HIS, FCS, ENG and GSGW have access to control communications and Ethernet based open communications to ease integration of CS 3000 with other systems.

4.4.4 Access Control Utility

System access is set by a user with system administrator privileges. Security is split into three separate functions (Engineering, Report, & Recipe management) as introduced in section 4.4.1. These three functions can be further broken into the following 5 access control tasks:

(1) System Administration
(2) Process Data Reporting
(3) Process Operation and Monitoring System
(4) Maintenance Builder
(5) Recipe Management

User Administration

User ID administration is broken into 3 administration sets: Engineer Function, Report function, and Recipe Management. Each set consists of its own, independent User IDs and groups. User IDs are assigned, and maintained, by the system administrator and passwords are set by the user at the time of first logging on.

The security system has these features:

(1) HIS User IDs can contain up to 16 alphanumeric characters with a maximum of up to 250 valid users.
(2) CS 3000 has a capacity of 50 user groups (with up to 8 alphanumeric characters).
(3) Each user must be belong to at least one user group.
(4) ENG User IDs can contain up to 16 alphanumeric characters.
(5) A minimum password length is configurable by the system administrator.

The following are configurable and should be set, per user SOPs, in order to maintain compliance to Part 11:

(1) Password expiration – a user will be notified of password expiration 14 days prior to password expiration via a prompt after logging onto the HIS or ENG.
(2) Account lockout – a user will be locked out of the ENG or HIS after a configurable amount of authentication failures. Notification of this lockout is also configurable. With optional packages, the alarm message can also be sent to PDA or mobile phone at real time.
(3) Screen Lock – the computer will be locked after a configurable time period has passed without user activity.

(4) Desktop environment - selectable between Windows or CENTUM desktop. The CENTUM desktop restricts the user from accessing the operating system and files on removable media (i.e. CD Rom, 3.45" floppy drives, etc.).

(5) The system offers a standard "OFFUSER" account, often used as the default account. This user account has configurable access privileges limited to the plant safety operations such as emergency shutdown and plant monitoring. There are two methods to use this account, both are configurable and not required to be used:

   a. The 'OFFUSER' account may be configured to be automatically logged on when starting the HIS.

   b. The, 'OFFUSER' can also be configured to be the default account when other user accounts are logged out due to inactivity.

(6) System administrators may set user accounts so the User ID can not be re-used at a later date. This feature satisfies Electronic Signatures (Subpart C) § 11.100 (a) of Part 11 preserving the uniqueness of each electronic signature

CENTUM Desktop Environment

The CENTUM desktop environment may be used to restrict access on HIS stations to only CS 3000 displays. This feature prevents operators from accessing standard Windows features such as Windows Explorer to directly access the file system. Using the CENTUM Desktop Environment system security is enhanced and the chance of accidental mistakes, such as file deletion, are prevented. The CENTUM Desktop Environment has the following features;

(1) Hide Windows Explorer

(2) Hide all the icons on the desktop

(3) Disables context menus

(4) Prevents access to the CD-ROM drive

(5) Disables use of [Ctrl] + [Alt] + [Del] key sequences

(6) Start menu restricted to only Yokogawa menu items

4.4.5 Electronic Records

The CS 3000 distributed control system is capable of generating a variety of electronic records for process historical reports, operator logs, trends, audit trails, and more.

CS 3000 assembles data, alarms, messages, and other electronic information in a secure environment and is considered to be the point of creation of the electronic records. The CS 3000 distributed control system is configured and maintained in an environment controlled by the end user and governed by applicable user policies and procedures. Access to the CS 3000 HMI is limited to authorized personnel with predefined privileges. These individuals have authorization to control their associated task(s) within the manufacturing process. In accordance with the definition in 11.3 (b) (4), CS 3000 is a closed system for the purpose of limiting access and maintaining integrity of electronic records.

In the Detailed Part 11 Compliance table, the provisions of Subpart C (Electronic Signatures) are described regarding personnel authentications.

Electronic records can be exported into common file formats that are suitable for long term storage and ready for review and evaluation. These formats are:

a) Audit Trail: PDF
b) Trend Data: CSV, Binary archiving
c) Reports: CSV, XLS, PDF
d) Master Recipe: PDF (using self-documentation package)

Using Exaquantum/Batch (Yokogawa's Batch PIMS) the control recipes and various production result data can be stored in a RDB. Exaquantum security may be configured so that neither the Report Package nor Microsoft Excel may be used to alter the data in the database. For more information refer to the "Achieving 21 CFR § 11 Compliance using Exaquantum/Batch" whitepaper available from Yokogawa and Stelex.

Audit Trail

Operations performed by users, on both the ENG and HIS, are subject to an audit trail. The audit trails are stored as electronic records and must be configured to be enabled. The tasks performed by operators are recorded in the audit trail containing information answering Who, When, Where, What, Why, and How.

The audit trail should be stored on a remote PC or server with adequate security. The PC or server should utilize redundant storage schemes and disk backup schedules.

Each record in the audit trail has a time stamp from the originating computer. The time of each computer in the CS 3000 system is automatically synchronized with a time master. The time master may be automatically selected by the system or set but the user when an external time source is used.

All operations performed at the HIS are recorded in the audit trail. Operational actions performed on the ENG such as starting / stopping of the audit trail and maintenance builders, saving of files, recipe maintenance and downloading to the HIS are recorded in the audit trail. Configuration specifics performed on the ENG are not detailed within the Engineer or Recipe Management Audit Trail Databases. Users must maintain an administrative management of change program to record configuration changes. CS 3000 configuration files may be are modular in nature and may be saved to aid with management of change, the engineering tools also permit most of the configuration data to be saved as ASCII files for management of change purposes. .

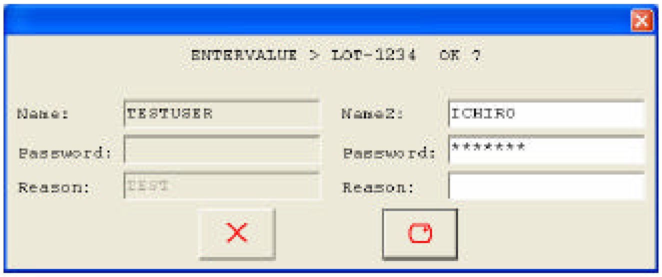
4.4.6 Electronic Signature

Electronic signatures are established to eliminate the need to print electronic records that are otherwise secure and compliant with regulations in Subpart B, solely for the purpose of uniquely identifying the individual that creates, manages, reviews, or approves content. CS 3000 systems employ User ID (user name) and password combinations as electronic signatures associated with individual electronic records. Standard on all CS 3000 systems are levels of user identification with password protection and configurable levels of secure access. Options are also available for identification through the use of third-party biometric devices (e.g. finger printing) for the purpose of executing electronic signatures.

For the electronic signatures of reports, such as daily reports or batch reports, the signature features of Acrobat may be used.

Double Authentication

For critical operations requiring second person verification, double authentication is available. The users performing a double authentication can be any authorized user. Default user accounts (e.g. ENGUSER, ONUSER, OFFUSER) are not permitted to perform authentication. Figure 2 shows a sample dialog box used to enter the double authentication.



ENTERVALUE > LOT-1234 OK ?

Name: TESTUSER
Password:
Reason: TEST

Name2: ICHIRO
Password: *******
Reason:

Figure 2 – Double Authentication Dialog Box

4.4.7 Report package

The data collected in a HIS such as process trend and closing data can be retrieved using Microsoft Excel and exported as reports in XLS, PDF, or CSV format. The report generation, modification, and export are all under access control and subject to audit trails if so configured using the Part 11 Report package.

The digital signature capability of Adobe Acrobat products can be used for the PDF files as the electronic signatures of the electronic records.

5 CENTUM CS 3000 - DETAILED PART 11 COMPLIANCE

The Detailed Part 11 Compliance Table is presented in this section. It analyzes each of the Part 11 requirements with reference to CS 3000 by means of a side by side discussion of the Part 11 requirements versus CS 3000 functionality.

All sections of the Part 11 regulation are included for reference and completeness, even if no analysis is required or even possible. Subpart A of Part 11 defines the scope, implementation, and definitions of Part 11. These sections are provided mainly for information and understanding of the regulation's requirements provided in Subparts B (Electronic Records) and C (Electronic Signatures).

Part 11 applies to all computer systems that create. modify, maintain, archive, retrieve, or transmit electronic records required by FDA regulations as well as systems used for electronic record submissions to the Food and Drug Administration (FDA). These regulations apply to the CS 3000 Human Machine Interfaces (including standard HIS stations, Recipe Development Stations, Engineering/Builder Stations, and Remote Reporting Stations). CS 3000 Human Machine Interfaces (HMI) are commercially available personal computers / workstations with Microsoft Windows operating systems and off-the-shelf configurable Yokogawa CS 3000 software applications.

The compliance of CS 3000 functionality to the Part 11 requirement is presented in the following three methods:

(1) Yes – CS 3000 supports the Part 11 requirement. User must create procedures for utilizing and maintaining the functionality.

(2) N/A – User must comply with requirement through SOP. These are instances where the user must develop and implement procedures specifically to meet these requirements.

(3) Shaded Cells – These are headings, titles, blank cells, etc. A cell containing CS 3000 Functionality of Part 11 requirements, whose compliance is determined as N/A, is also shaded.

As with the installation of any system, validation is the responsibility of the user. The user must implement a system life cycle methodology, policies and procedures thoroughly and appropriately. Yokogawa aides in this arduous process by providing the comprehensive and compliant CS 3000 product.

5.1 General Provisions (Subpart A)

§11.1 Scope

(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.

(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with §11.2, unless paper records are specifically required.

(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

§11.2 Implementation

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

(1) The requirements of this part are met; and

(2) The document or parts of a document to be submitted have been identified in public docket No. 92S–0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

§11.3 Definitions

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:

(1) Act means the Federal Food, Drug, and Cosmetic Act (secs. 201–903 (21 U.S.C. 321–393)).

(2) Agency means the Food and Drug Administration.

(3) Biometrics means a method of verifying an individual’s identity based on measurement of the individual’s physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

(4) Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

(5) Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

(6) Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is

created, modified, maintained, archived, retrieved, or distributed by a computer system.

(7) Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

(8) Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

(9) Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

5.2 Electronic Records (Subpart B)

Section #	Requirement	Compliance		CS 3000 Functionality
		Yes	No	
§ 11.10 Controls for closed systems.				
	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:			CS 3000 must be configured as a closed system for the purpose of limiting access and maintaining the integrity of electronic records. Secure methods for operator and engineer access to the four major operations (Process Operation, Builder Maintenance, Process Data Reporting and Master Recipe Maintenance) are designed in accordance with Part 11.
(a)	**Validation of systems** to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. **NOTE:** The FDA intends to exercise enforcement discretion regarding this requirement for Part 11, though persons must still comply with applicable predicate rule requirements for validation. The FDA recommends that validation be based on a justified and documented risk assessment.	YES		Validation of CS 3000, as with any system, is unique to each installation due to specific user requirements and is ultimately the user's responsibility. Validation of CS 3000 systems is performed in accordance with the end user's master validation plan. All process operations are recorded automatically by the system Audit Trail, if so configured. Moreover, all operations performed for process Data Reporting, Builder Maintenance and Master Recipe Maintenance are also automatically recorded by the system Audit Trail function.

Section #	Requirement	Compliance		CS 3000 Functionality
		Yes	No	
(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. **NOTE:** The FDA intends to exercise enforcement discretion regarding this requirement for Part 11; persons should provide an investigator with reasonable and useful access to records during an inspection ensuring the copying process produces copies that preserve the content and meaning of the record.	YES		In consideration of this requirement for portability, security, and traceability, electronic records can be exported into common file formats, suitable for long term storage and ready for review and evaluation by the FDA. These formats are: 1. Audit Trail: PDF 2. Trend Data: CSV, Binary Archiving 3. Reports: CSV, XLS, PDF 4. Master Recipe: PDF (Using self-documentation package) Using Exaquantum/Batch, Yokogawa's Batch PIMS, the control recipes and various production result data can be stored in an RDB. Exaquantum security may be configured so that neither the Report Package nor Microsoft Excel may be used to alter the data in the database.
(c)	**Protection of records** to enable their accurate and ready retrieval throughout the records retention period. **NOTE:** The FDA intends to exercise enforcement discretion regarding this requirement for Part 11. The FDA suggests the decision on how to maintain records be based on predicate rule requirements and on a justified and documented risk assessment.	YES		Audit trail functionality is provided with a viewer to provide the ability to efficiently search for required electronic records. With this viewer, electronic records can be efficiently queried according to their date, personnel, batch ID, equipment, message type, or some arbitrary text string using the filter feature. The results of this search and search condition (meta-data) can be exported into a read-only PDF file. When saving the data of the audit trail, the free space of the hard disk is checked.

Section #	Requirement	Compliance		CS 3000 Functionality
		Yes	No	
(d)	**Limiting system access** to authorized individuals.	YES		System access limitations are provided for : 1. System Administration 2. Process Data Reporting 3. Process Operation and Monitoring System 4. Maintenance Builder 5. Recipe Management Personnel Authentication is performed using user ID and password. Authentication is required at login, and can be configured to be required for performing desired actions. The system administrator assigns access privileges to users based on user defined requirements. The system offers a standard “OFFUSER” account, often used as the default account. This user account has configurable access privileges limited to the plant safety operations such as emergency shutdown and plant monitoring. There are two methods to use this account, both are configurable and not required to be used: (1) The ‘OFFUSER’ account may be configured to be automatically logged on when starting the HIS. (2) The, ‘OFFUSER’ can also be configured to be the default account when other user accounts are logged out due to inactivity. Access to the operating system, Windows Explorer, and files on removable media (CD Rom and 3.45” floppy drives) are restricted by CENTUM Desktop functions.

Section #	Requirement	Compliance		CS 3000 Functionality
		Yes	No	
(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. NOTE: The FDA intends to exercise enforcement discretion regarding this requirement for Part 11, though persons must still comply with applicable predicate rule requirements related to documentation of, for example, date, time, or sequencing of events. FDA states even if no predicate rule exists for this requirement, it may still be important to have audit trails or other security measure to ensure the trustworthiness and reliability of the records.	YES		By default the system automatically maintains a history of operator entries and actions. Audit trail entries contain information answering: Who, When, Where, What, Why and How whenever the data is available and applicable. Audit trail entries also contain the new and previous value to prevent previously recorded information from being obscured. All operations performed at the HIS are recorded in the audit trail. Operational actions performed on the ENG such as starting / stopping of the audit trail and maintenance builders, saving of files, recipe maintenance and downloading to the HIS are recorded in the audit trail. Configuration specifics performed on the ENG are not detailed within the Engineer or Recipe Management Audit Trail Databases. Users must maintain an administrative management of change program to record configuration changes. CS 3000 configuration files may be are modular in nature and may be saved to aid with management of change, the engineering tools also permit most of the configuration data to be saved as ASCII files for management of change purposes. Each record in the audit trail has a time stamp from the originating computer. The time of each computer in the CS 3000 system is automatically synchronized with a time master. The time master may be automatically selected by the system or set but the user when an external time source is used. The audit trail is stored in a database separate from the operational data. The audit trail is retained as part of the CS 3000 database and may be available for as long as the subject electronic records are preserved. It can also be sorted and then exported to a PDF file.

Section #	Requirement	Compliance		CS 3000 Functionality
		Yes	No	
(f)	**Use of operational system checks** to enforce permitted sequencing of steps and events, as appropriate.	YES		Standard sequence functions provided in the CS 3000 systems can be configured to enforce permitted sequencing of steps and events as needed. The following sequence functions can be used to enforce the permitted operations steps: 1. SFC 2. Sequence Table 3. Logic Chart 4. SEBOL
(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.	YES		CS 3000 has the capability to perform authority check. This may be configured as part of the engineering development. Authority checks may be performed for many different system features such as function blocks, displays, messages, and control recipes. Each authority check may be assigned a required authorization level. There are seven authorization levels such as "Read-Only", "Read/Write", Operator console (HIS) capabilities: The operation windows, function blocks and messages displayed on each operator console can be assigned different authorization levels required for access. Likewise restrictions on each operation group can be also be enforced. The system can be configured to require a user to enter an electronic signature (user ID and password) to confirm their identity when performing certain actions to positively identify the person taking the action. Each user account is assigned to an individual and given specific privileges by a System Administrator. Normal users of the system do not have the ability to access these features.

Section #	Requirement	Compliance		CS 3000 Functionality
		Yes	No	
(h)	**Use of device** (e.g., terminal) **checks** to determine, as appropriate, the validity of the source of data input or operational instruction.	YES		Field I/O devices (I/O modules) connected to the CS 3000 are wired to the system. The movement of these devices should be under configuration control as it the CS 3000 configuration. Therefore the actions taken with connected devices occur at known locations. All the audit trail entries recording operations performed from operator consoles (HIS) are stamped with the console ID and the user ID used to perform the operation, along with a timestamp documenting when the audit trail entry was recorded.
(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.	N/A		Users are responsible for developing, implementing, and maintaining their own training programs and establishing criteria for the determination of qualifications of persons who develop, maintain, and/ or use CS 3000 and 21 CFR Part 11. A proper education program according to the work assignment of each individual is required. The execution of the education program should be recorded. Yokogawa offers standard and custom training classes on the development, maintenance, and use of CS 3000 system features. The engineering tasks of CS 3000 should be performed by personnel that have had the proper training as stipulated by the company rules.
(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**.	N/A		Users are responsible for developing, implementing, maintaining and enforcing their own written policies and procedures. Strict adherence to effective and practical policies and procedures ultimately affects the quality of the final product.
(k)	Use of appropriate controls over **systems documentation** including:			

Section #	Requirement	Compliance		CS 3000 Functionality
		Yes	No	
(1)	**Adequate controls** over the distribution of, access to, and use of documentation **for system operation and maintenance**.	N/A		Yokogawa maintains control of Cs 3000 documentation as it is developed and maintained. Upon receipt of CS 3000 documentation users are responsible for controlling the documentation by establishing and maintaining an effective documentation management system.
(2)	**Revision and change control procedures** to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	YES		Yokogawa controls the development, maintenance and distribution of CS 3000 documentation within Yokogawa and to its customers. CS 3000 has self-documentation capabilities. This feature may be used to support the documentation of configuration. CS 3000 self-documentation can add a revision number for audit trail purposes when outputting to paper document or to PDF file. End users must incorporate CS 3000 configuration activities into their management of change systems and document control systems.

Section #	Requirement	Compliance		CS 3000 Functionality
		Yes	No	
§ 11.30 Controls for open systems				
	Persons who use open systems to create, modify, maintain, or transmit electronic records **shall employ procedures and controls** designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall **include those identified in § 11.10,** as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	N/A		CS 3000 must be used as a closed system in which system access must be configured to ensure compliance to Part 11. Procedures and policies must be developed, implemented, maintained and enforced to also ensure this compliance.

Section #	Requirement	Compliance Yes	Compliance No	CS 3000 Functionality
§ 11.50 Signature Manifestations				
(a)	**Signed electronic records** shall contain information associated with the signing that clearly indicates all of the following:			
(1)	The printed name of the signer	YES		The user name is authenticated in real time by checking the user ID name (User-In dialog box) against the registered user names in the Security Builder. The name can also be put in the remarks column of the audit trail. Audit trail entries contain the user's ID. User IDs may be mapped to a person's full name by exporting the ID/Name list using the self-documentation feature.
(2)	The **date and time** when the signature was executed; and	YES		Each record in the audit trail is time stamped with year, month, day, hour, minute, and second.
(3)	The **meaning** (such as review, approval, responsibility, or authorship) associated with the signature.	YES		Each record requiring electronic signature confirmation in the audit trail can contain a meaning/ reason field for entry by the user at the time of confirmation.
(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).	YES		The audit trail can be viewed electronically and can be exported to a PDF file (by self documentation).

Section #	Requirement	Compliance		CS 3000 Functionality
		Yes	No	
§ 11.70 Signature/record linking				
	Electronic signatures and hand-written 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		User ID's are automatically included in the Audit Trail by the CS 3000 system within the relevant electronic records as they are generated. Audit trail entries contain the user's ID. User IDs may be mapped to a person's full name by exporting the ID/Name list using the self-documentation feature. Audit Trail files are generated as write protected system files.

5.3 Electronic Signatures (Subpart C)

Section #	Requirement	Compliance		CS 3000 Functionality
§ 11.100 General requirements				
(a)	Each **electronic signature shall be unique** to one individual and shall not be reused by, or reassigned to, anyone else.	YES		The system administrator maintains the User IDs and sets the initial password. Each user should change their own password to make it confidential. Once a User ID becomes invalid (retire, transfer), as set by the administrator, the User ID cannot be used again. This feature is available with the installation of the Access Administration Package and is configurable.
(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**.	N/A		Users are responsible for administration of user accounts. Policies and procedures have to be implemented to meet this requirement.
(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.	N/A		Users are responsible to certify to the agency that the electronic signatures in their system are intended to be legally binding. This should be done prior to utilizing electronic signatures in their system and only after the agency recognizes that the certification is complete.

Section #	Requirement	Compliance		CS 3000 Functionality
(1)	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.	N/A		Users are responsible to ensure that this certification is forwarded as specified by the agency.
(2)	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.	N/A		Users are responsible to provide any additional evidence and testimony, as requested by the agency, that a specific electronic signature is legally binding. The agency should be convinced of this testimony prior to utilizing the electronic system.

§ 11.200 Electronic signature components and controls				
(a)	Electronic signatures that are not based upon biometrics shall:			
(1)	Employ **at least two distinct identification components** such as an identification code and password.	YES		CS 3000 electronic signatures use user ID and password for authentication of individuals. The user ID is a unique string of up to 16 alphanumeric characters assigned by the system administrator. The password is a user (system administrator) defined string of up to 32 alphanumeric characters assigned by the individual user.
(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.	YES		CS 3000 requires both user ID and password be entered when first logging into a HIS or ENG station.. If a series of actions requiring an electronic signature are taken, both components of the signature are required initially (i.e. both the user ID and the user's password). Only the User's Password need be entered for subsequent signings. If an HIS is inactive for a configurable period of time, the current user will automatically be logged out.
(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.	YES		If the user is logged out either manually or automatically, further operations cannot be performed until the user logs in again. Both user ID and password are required to be entered in the User-In dialog box for re-authentication .
(2)	Be used only by their genuine owners.	YES		Users are responsible for administration of user accounts. The password of a user is set the first time that a user logs onto the system. The password should not be disclosed to anyone, not even the system administrator. Policies and procedures must also be implemented to meet this requirement.

(3)	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.	YES	▨	Using an individual electronic signature by anyone other than its genuine owner requires an 'OnBehalf' signature, and the OnBehalf users procedure should be established. For example, the On Behalf signature should be performed with the collaboration of the On Behalf user and system administrator. A user should have a password in CS 3000 system that cannot be easily guessed or parsed by others. In case emergency actions are required and the person assigned for the required actions is absent, another person having the same or higher privileges is able to take the actions on behalf. Using a mode-switching key (physically a metal key), an operator can switch into a special user "Engineer" who has a higher privilege to perform almost all operations. Nevertheless, all the operations performed by "Engineer" is logged and recorded by audit trail. Since the computer cannot identify the particular individual that performed the operations under the account of "Engineer," it is necessary to have a security policy on the management of the mode-switching key.
(b)	**Electronic signatures based upon biometrics** shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	YES	▨	Fingerprint identification unit is available as an option for user authentication.

§ 11.300 Controls for identification codes/passwords

	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:			
(a)	**Maintaining the uniqueness of each combined identification code and password**, such that no two individuals have the same combination of identification code and password.	YES		Users are responsible for maintaining this uniqueness. The system checks for the duplication of a user's ID when the administrator adds a new user to the system and does not allow duplicate user ID's. Each user has their own password, which is set by the user and unknown to the administrator. Once a User ID becomes invalid (retire, transfer), as set by the administrator, the User ID cannot be used again.
(b)	Ensuring that **identification code and password issuances** are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	YES		The system administrator maintains the User IDs. Both the Windows Operating System and CS 3000 have password validity period warnings and checks. When the expiration date is past, the system prompts for updating the password.
(c)	**Following loss management procedures** to electronically de-authorize 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.	YES		When a specific User ID becomes invalid (due to compromised password, retirement, or other), the User ID is marked invalid by the authorized administrator. Invalid ID's are not deleted, but are maintained by the system to prevent future reuse. This is a feature of CS 3000 Access Administration Package and must be configured accordingly.

(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.	YES		When a user logon fails repeatedly (configurable amount of attempts) an authentication failure alarm message may be broadcast to all alarm terminals (i.e. HISs) and the event is recorded in the audit trail. The offending user ID will be locked out (User Lockout feature). With optional packages, the alarm message can also be sent to a PDA or mobile phone in real time.
(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.	N/A		Security settings can be checked and confirmed during the computer validation, initially and periodically as needed. Policies and procedures should be implemented to ensure that this is performed.

Yokogawa:

Yokogawa's global network of 18 manufacturing facilities, 69 affiliate companies and over 200 sales and engineering offices span 28 countries. Since its founding in 1915, the US$3 billion company has been engaged in research and innovation of the highest order, securing over 4,500 patents and registrations, including the world's first DCS and digital flow and pressure measurement sensor. Industrial Automation Systems, test and measurement systems and information services are a core business of Yokogawa. For more information about Yokogawa Electric Corporation please visit their website at www.yokogawa.com

Stelex:

Stelex provides enterprise-wide compliance solutions to regulated industries in the Pharmaceutical, Medical Device, Diagnostic and Biotechnology sectors. The firm delivers a comprehensive suite of Validation, Technology, Regulatory and Business solutions. Services include Computer System Validation, Process Validation and Equipment Qualification, Infrastructure Qualification, Laboratory Systems Validation, Automation and Controls Validation, System Integration, Implementation and Software Development, as well as Security and PKI services, Quality Assurance, Auditing, Program Management and Best Practice Consulting. In addition to technical training and professional education provided through its accredited Stelex University, Stelex offers ComplianceBuilder, the compliance infrastructure solution. To learn more, please visit us at www.stelex.com