C TECHNOLOGIES, INC.
A REPLIGEN COMPANY

Solo VPE

White Paper

21 CFR Part 11 Compliance Position for the SoloVPE® System

SoloVPE Software Suite Version 3.X.YYY

Slope spectroscopy®

Document Number: DOC0160
Revision Number: 01 09/17/2020

C Technologies, Inc. Corporate Office:

C Technologies, Inc. (Global Headquarters) 685 Route 202/206 Bridgewater, NJ 08807 USA

International telephone:	+1 908-707-1009
International fax:	+1 908-707-1030
Applications email:	analytics-applications@repligen.com

The C Technologies, Inc. homepage can be found at www.ctechnologiesinc.com

All Things Legal:

C Technologies, Inc. is the owner of copyrights on this document and the associated Software. Under the law, the written permission of C Technologies, Inc. must be obtained before either the documentation or the software is copied, reproduced, translated, or converted to electronic or other machine-readable form in whole or in part.

Agilent Inc. is the owner of the copyright on the Cary WinUV documentation and associated software. Under the law, the written permission of Agilent Inc. must be obtained before either the documentation or the software is copied, reproduced, translated, or converted to electronic or other machine-readable form, in whole or in part.

SoloVPE® is a registered trademark of C Technologies, Inc.

Slope Spectroscopy® is a registered trademark of C Technologies, Inc.

Microsoft Windows® is a registered trademark of Microsoft Corporation.

Abstract

Compliance with 21 CFR Part 11 requires that procedural and administrative controls be put in place by an organization in addition to the technical controls that are available in software packages. This includes validating the electronic records system, drafting and maintaining standard operating procedures for the use of the electronic records system, and ensuring that users of the electronics records system have adequate training regarding its appropriate use, administration, and role in maintaining compliance.

The SoloVPE® System (comprising the Microsoft Windows operating system, Agilent Technologies Cary WinUV spectroscopy Environment, and C Technologies, Inc. SoloVPE software) provides compliance with the FDA's ruling on electronic records and electronic signatures. As the capabilities and functions available in the software alone cannot guarantee a compliant implementation, the procedural controls set by the organization are responsible for proof of compliance.

In relation to the complexity of each organization's policies and the FDA's regulations, C Technologies, Inc. provides training and online support to assist customers in understanding the full capabilities of the SoloVPE System and closing any potential compliance gaps.

Introduction

Title 21 CFR Part 11 of the Code of Federal Regulations set by the United States Food and Drug Administration sets the criteria for which electronic signatures, electronic records, and handwritten signatures executed to electronic records to be considered trustworthy and reliable.[1] It provides the guidelines and rules related to copying, permissions, audit-log tracking, version control, and the application of electronic signatures to electronic documents.

This paper is intended to provide information about the tools, capabilities, and functionality available in the SoloVPE software for organizations considering the implementation of a 21 CFR Part 11 compliance system. Ultimate responsibility for achieving full compliance with the 21 CFR Part 11 requirements lies with the customer's criteria, implementation, and validation processes and efforts. Nevertheless, C Technologies works with its customers to assist them in understanding any software limitations and, at its discretion, incorporates possible enhancements.

The full text of 21 CFR Part 11 can be found on the Electronic Code of Federal Regulations website: https://www.ecfr.gov

[1] U.S. Department of Health and Human Services, Food and Drug Administration, Center for Drug Evaluation and Research, Center for Biologics Evaluation and Research, Center for Devices and Radiological Health, *Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11 – Questions and Answers: Guidance for Industry* (June 2017), https://www.fda.gov/ media/105557/download.

1. Background

A successful implementation of the System requires a complete understanding of the capabilities of the software. A complete understanding of the software requires a comprehensive appreciation of the infrastructure of the software environment. In the case of the SoloVPE System, the software platform is constructed from three major components:

- Microsoft Windows Operating System
- Agilent Technologies Cary WinUV Spectroscopy Environment
- C Technologies, Inc. SoloVPE Software

These three core components work cooperatively to create a complete interface for command and control of the SoloVPE hardware. The Cary WinUV spectroscopy software suite is a complete spectroscopy workbench that was designed to control Agilent's line of Cary spectrophotometers. The platform provides direct control and configuration of the various hardware systems and their respective accessories creating a common user interface for the development of methods and the acquisition, analysis, and presentation of data both graphically and in reports. It has an array of options that enable the retention and retrieval of data in a number of different file formats. The SoloVPE software is integrated seamlessly with the Cary WinUV platform since the functional overlay of the variable pathlength capabilities was designed and engineered using Agilent's proprietary Advanced Development Language (ADL) spectroscopy authoring command set. It exists only and exclusively within the Cary WinUV software environment and leverages the core capabilities of the Agilent Cary WinUV platform.

For secured implementations of the SoloVPE System, C Technologies recommends the implementation of the SecureVPE software application. The SecureVPE software works in conjunction with the security capabilities of the network environment and the SoloVPE Administration parameter settings to create a powerful-yet-flexible set of security tools.

The balance of this document includes more detailed information regarding how these components work together, the specific roles each plays, and some examples and options of how they can be used to achieve a compliant implementation. The three security layers used to achieve compliance with 21 CFR Part 11 include Windows NTFS, SoloVPE Administration, and SecureVPE.

2. Specific Applications

This section of the document provides more detailed information as to how the tools available in the SoloVPE System can be applied to the relevant section of the 21 CFR Part 11 regulations by companies as part of an overall compliance plan.

2.1 §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:

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

C Technologies provides qualification services in the form of Installation Qualification Operational Qualification (IQOQ) of the SoloVPE System by trained VPT Support Specialists. This service is included when Systems are purchased to ensure that the hardware and software are properly installed at the customer location. Following the IQOQ, the customer can begin to develop the required policies and procedures and utilize the tools available with the System in accordance with the compliance plan.

Preventative Maintenances (PMs), which include an IQOQ, can be purchased to ensure optimal and consistent performance of the System. C Technologies does recommend periodic requalification of the system and does offer periodic PM services to SoloVPE owners.

Audit trails in the System provide detailed information regarding system access, performance, use and manipulation to help customer comply with the regulation. Invalid or altered records are captured and stored within the audit trails. Audit trail information is available in multiple layers of the System:

- Event Logs and Network Logging can be configured by the customer to control and monitor access.
- The Agilent Cary WinUV environment maintains a detailed method audit trail that is saved with each data file.
- The VPE Audit Viewer comprises a general audit log, a SecureVPE audit log, an extinction coefficient audit log, and an eSignature audit log.

(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.

The Agilent Cary WinUV environment is a complete spectroscopic software platform designed to work with the Cary line of spectrophotometers. It has within it the ability to capture, analyze, report, and save spectroscopic data. There are several proprietary file formats (Batch, Data, Method, Report, and Grams) that the System can create electronically as well as more common files (.CSV and .RTF). Widely available programs that produce portable document formats such as PDF and XPS, can also be produced when they are installed on the computer system. Hard copy output is also an option when a physical printer is connected to the system. To ensure accurate audit trail tracking and compliance with save path locations, it is highly recommended to save data as a batch file (.BVP) through the SoloVPE software.

The ability to create, save, modify, and delete these electronic records can be controlled through the customers' appropriate and supportive use of workstation and NTFS file and folder permissions. The customer is responsible for establishing proper user and group permissions and incorporating their use into the workflow and standard operating procedures.

(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

The ability to create, save, modify, and delete electronic records created with the SoloVPE System can be controlled through the customers' appropriate and supportive use of workstation and network file and folder permissions. The customer is responsible for establishing proper user and group permissions and incorporating their use into the workflow and standard operating procedures. Customers must decide which file formats are appropriate for their compliance plan and then develop a supportive file and folder permissions approach with the tools that are provided on the SoloVPE System and their own network infrastructure.

(d) Limiting system access to authorized individuals.

Access controls to the SoloVPE System can be set at all three levels of the software to some extent. Each layer provides unique options and functionality that the customer should consider when developing a compliance plan.

The following table provides a basic overview to give guidance on how to incorporate these features a compliance plan.

Layer	Access Control Overview
NTFS Permissions	• NTFS permissions can be controlled on folders and files by setting user and group permissions at the customer's discretion. Microsoft provides significant flexibility in establishing security profiles. Configuring these features requires the knowledge and experience of a trained IT professional. • When customers choose to connect the SoloVPE System computer to a network domain, even more complexity and options for securing the system become available. A network administrator familiar with the compliance plan will be required to ensure that the customer's policies and procedures have been appropriately implemented. • The security controls available in the operating system and network afford customers tremendous flexibility to controlling access to the SoloVPE System such as log on monitoring, password group policies, log on attempt tracking and lock out.
SoloVPE Administration	• The SoloVPE Administration program contains device information, settings, support files and software licensing. This application gives the user the ability to configure details specific to the organization as well as the device. • SoloVPE Administration contains an optional feature called the VPE System Service. This feature is used to overcome ownership of local files, unsecured WinUV options and uncontrolled ADL closing during a user lockout. The VPE System Service runs in the background, contains no user interface and searches for events that require it to act. • A complete exploration of the parameter settings available in the SoloVPE Administration program is beyond the scope of this document. However, it is crucial to understand that the controls provided at this layer of the security structures relate exclusively to the SoloVPE software and need to be configured in conjunction with the other layers to meet the goals of the organization.
SecureVPE	• The SecureVPE application is an optional security module and a companion product to the SoloVPE software. • SecureVPE links directly to the Windows Active Directory data store for user and group data at both the local machine and the domain level. This allows single-user and group policies, password policies, and related local policies to be administered by the organization's IT and administrative staff.

(Table continued on next page.)

Layer	Access Control Overview
SecureVPE	• The SecureVPE application provides a specific security matrix that relates specifically the SoloVPE software. The permissions options have been designed to provide the customer and the Administrator control over access to specific features and functions in the SoloVPE environment. In some cases, permission settings may toggle a button state between enabled and disabled, or visible and invisible. In other cases, permissions settings may provide for or revoke the option of performing a certain task, such as performing an electronic signature or whether the Auto Save functionality is enabled. • A complete exploration of the permission settings available in the SecureVPE application is beyond the scope of this document; however, they can be reviewed in the SecureVPE User Manual DOC0119. It is critical to understand that the controls provided at this layer of the security structures relate exclusively to the SoloVPE software and need to be configured in conjunction with the other layers to meet the goals of the organization.

(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.

Extensive audit trails are recorded within the various levels of the SoloVPE software environment. Customers have extensive options for the configuration of both the computer workstation and the network domain including the tracking of actions by user and the various Event Logs that exist within the Windows operating system.

Audit trails related to the data or method reside in the actual batch (*.BPV) or method (*.MVP) files. The Trace Preferences button allows the user to access all raw data and method audit trails.

The VPE Audit Viewer is not secured via the User Account Control settings (UAC) because the application provides read-only viewing of the audit trail information. It provides a single source for reviewing specific audit trails and ensures accessibility, even without administrative privileges. The four types of audit log information are described as:

- **General Audit Viewer:** Provides an overview of when, what, and who performed actions within the SoloVPE software.
- **SecureVPE Audit Viewer:** Provides an overview of when, what, and who performed actions within the SecureVPE software.

- **Extinction Coefficient Audit Viewer:** Provides an overview of when and who populated all extinction coefficients added to the EC database.
- **ESignatures Audit Viewer:** Provides an overview of when and how eSignatures are triggered within the SoloVPE software.

The extent to which a customer makes use of these capabilities must be decided by the organization and be implemented with their own internal network experts. These decisions need to include their plan for maintaining, backing up and archiving data.

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

C Technologies recommends the organization develop policies and procedures that utilize the capabilities and functions within the SoloVPE software to enforce the permitted sequencing of steps and events using operational system checks. The security features of the SoloVPE software, particularly the SecureVPE, allow customers to setup up users and groups with specific permissions to create, modify, and run methods. When permissions are properly configured, users are constrained by the method parameters and their SecureVPE permissions. Proper configuring of permissions combined with the automatic electronic signature capability allows the customer to ensure the integrity, and authenticity of the electronic record.

(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.

The SoloVPE System can be configured to authorize the following: access to and control of the System, configuration or record changes, and electronic signatures. The organization is responsible for designing the policies and procedures around the System’s capabilities in order to meet their compliance goals. Because there are multiple layers of security features, it is important to consider the specific features available within each layer when designing the security plan. Each layer can be configured to secure specific types of access, control, and data.

The Windows operating system and the network architecture are an integral part of any security plan. Customers must involve their network administrator to successfully design and implement their computer/network security structure. Issues such as controlling the read, write, and modify permissions within the NTFS file system both on the work station and any accessible file servers are critical to ensure that records can be created, secured, and archived correctly.

C Technologies provides specific information regarding the security requirements of its software packages; however, it cannot provide guidance on the overall network security due to the complexity and variability existing in the industry. At the most basic level, however, Windows allows customers to configure unique user accounts that are password protected. The network administrator can control user access to the computer/network and an overall profile of their permissions. When implemented in this fashion, the Windows login creates a first line of defense for securing the computer system. The user profile can also be controlled as to where and how file data is created, saved, modified, deleted, or overwritten.

The SoloVPE Administration program is the second security threshold for the SoloVPE System. This program works in conjunction with the UAC, meaning that local administrator accounts and nonlocal administrator accounts can have access to the software. Only local administrator accounts can have access to the software if the UAC is set to Default or higher.

To prevent unauthorized use of the software, nonlocal administrator accounts are prompted for elevated credentials. However, when the UAC is set to Never Notify, local and nonlocal administrator accounts can have access to the software if granted within SecureVPE. The UAC makes it difficult for unauthorized users to change critical settings or gain control of the Windows and installed software. The SoloVPE software has been designed and built to leverage this powerful security feature. C Technologies recommends that the UAC be set to Default or higher to fully secure their SoloVPE System.

The final and more detailed level of security is controlled by the SecureVPE software. Similar to the SoloVPE Administration program, SecureVPE works in conjunction with the UAC Windows environment. The SecureVPE software enables the organization to configure a SoloVPE-specific permissions matrix for each user. The permissions that can be set using the SecureVPE software toggle access to specific features and functions within the SoloVPE software environment, providing administrators the flexibility to control what actions users perform when they access the System.

The SecureVPE software no longer relies on the GLP Administration program. It uses the Windows Active Directory to link directly to users and groups at both the local machine and the domain level. Additionally, the eSignature capability within the SoloVPE software is configured within the SecureVPE environment thus prompting the user to provide authenticated credentials to authorize critical steps in the process.

(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

The SecureVPE software can be configured to prompt the logged in user to record an eSignature through an authentication prompt. This requires the logged in user to provide their password before and after critical operations to ensure the validity of the input and output.

(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.

C Technologies has been supporting fiber-optic-based spectroscopy equipment in the bio-pharmaceutical industry for more than a decade. As part of its implementation of the SoloVPE System, an organization can contact C Technologies to request and review aspects of its development policies, processes, and procedures. C Technologies provides employee training and education in a variety of ways. Some of the services include on-site training, support webinars, user documents, and phone support.

(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.

C Technologies recommends that the organization develop policies and procedures that describe and govern the actions that administrators and end users must perform using the SoloVPE System. For administrators, policies and procedures should be developed for system-related actions such as user and group management, password management, and SecureVPE user permissions. For end users, policies and procedures should be developed for actions such as method creation, data-naming conventions, and eSignature applications.

(k) Use of appropriate controls over systems documentation including:

(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

C Technologies provides documentation with each SoloVPE System. The documentation is updated and distributed with each version of the software. It is up to the organization to implement security controls over the access and use of the documentation.

2.2 §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.

C Technologies recommends that the organization implement appropriate policies and procedures, given the capabilities and constraints of the SoloVPE System, to achieve compliance with this requirement. The SoloVPE System and security capabilities provide specific functionality intended to support compliance as it relates to user authentication, data integrity, and confidentiality as follows:

Authentication: System access can be controlled through both the Windows operating system/network domain access as well as the SecureVPE program.

Integrity: Customers can configure various security levels to constrain the generation, modification, and storage of data by specific user accounts and electronic signatures. Customers can utilize the VPE Audit Viewer to view specific events that occurred within the software.

Confidentiality: To ensure confidentiality, C Technologies recommends that customers establish appropriate workstation and network security profiles that can control user-specific visibility and accessibility of information. Documented policies and procedures also need to be part of the implementation plan for the organization.

Digital Signatures: The SecureVPE software system allows for the implementation of account-driven electronic signatures. In addition to the automated prompts, the system can be configured to allow users to initiate electronic signature events for reviews and approvals.

2.3 §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;

(2) The date and time when the signature was executed; and

(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

Electronic signatures are executed by the user through the SoloVPE software application interface, whereupon the user is required to enter their username and password. The electronic signature is stored with the data in the batch file along with the signer’s full name, date, time the signature was executed, purpose of the signature (author, review, approval, or override) and reason for the signature. The user also has the option to append comments to the electronic signature at the time of execution.

(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).

The SoloVPE software appends a human readable text block with the details of each electronic signature. This information can save as an auditable batch file. Because it co-exists with the data, the security and control structure are identical.

2.4 §11.70 Signature/record linking.

Electronic signature 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.

The electronic signature, if applied, will append to the existing report. The collected data can be saved as a batch file, which will contain the established electronic signature. C Technologies recommends that the organization create the necessary policies and procedures, given the capabilities and constraints of the SoloVPE System, to achieve compliance with this requirement.

2.5 §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.

C Technologies recommends that the organization implement policies and procedures to ensure that user names are assigned to only one individual and that each individual agrees not to divulge their password under any circumstances. These policies and procedures must be applied to the Windows/network domain user names and the user must be given authorization to eSignatures within SecureVPE.

(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.

C Technologies recommends that the organization incorporate policies and procedures to ensure that usernames are assigned to individuals with proper authorization and approval given their role and responsibilities.

(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.

(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.

(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.

C Technologies recommends that the organization implement policies and procedures, given the capabilities and constraints of the SoloVPE software, to comply with the certification requirements of this regulation. It is up to the organization to certify that the electronic signatures create legally binding equivalents to traditional handwritten signatures.

2.6 §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.

(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.

(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.**

(2) Be used only by their genuine owners; and

(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.

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

The SoloVPE System does not use biometric authentication techniques. Instead, a user of the system enters their username and password to authorize a signature.

2.7 §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.

C Technologies recommends that the organization create policies and procedures to ensure the uniqueness of the identification code and password combinations. The Windows operating system and network domain management capabilities provide for extensive types of password policies including, complexity, aging, change requirements, lock out, reuse prevention and expiration. Organizations' should involve their network administrator to define policies that support their overall implementation plan.

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

C Technologies recommends that the organization create policies and procedures to ensure that identification codes and passwords are periodically reviewed and managed as required. The Windows operating system and network domain management capabilities provide for extensive types of password policies including complexity, aging, change requirements, lock out, re-use prevention, and expiration

(c) Following loss management procedures to electronically deauthorize 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.

C Technologies recommends that the organization create policies and procedures to ensure that identification codes and passwords are deauthorized, if required. The Windows operating system and network domain management capabilities provide for extensive types of password policies including complexity, aging, change requirements, lock out, re-use prevention, and expiration.

(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.

C Technologies recommends that the organization create policies and procedures to ensure that identification codes and passwords are safeguarded as required. The Windows operating system and network domain management capabilities provide for extensive types of password policies including complexity, aging, change requirements, lock out, re-use prevention, and expiration.

(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.

C Technologies recommends that the organization create policies and procedures to ensure that devices containing identification codes and passwords are periodically tested as required. The Windows operating system and network domain management capabilities provide for extensive types of password policies including complexity, aging, change requirements, lock out, re-use prevention, and expiration.

Conclusion

C Technologies is committed to working with its customers to successfully achieve the implementation and deployment of its technologies. The utility and broad applicability of UV-Vis measurements is reflected in the diversity of our customers and installation sites.

Many of our customers are in the bio-pharmaceutical industry and are subject to a variety of regulatory constraints. C Technologies is committed to working with our customers to ensure that the capabilities and functionality of its system enable customers to design and implement a compliance installation. To help successfully craft a compliance plan, C Technologies provides support services that highlight the tools, capabilities, and requirements of the SoloVPE System. Ultimately, compliance remains the responsibility of the customer.

References

U.S. Department of Health and Human Services, Food and Drug Administration, Center for Drug Evaluation and Research, Center for Biologics Evaluation and Research, Center for Devices and Radiological Health. Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11 – Questions and Answers: Guidance for Industry. June 2017. https://www.fda.gov/media/105557/download.