

# *Application Note*

LIGHTHOUSE

***FMS and 21 CFR  
Part 11 Compliance***

WORLDWIDE SOLUTIONS



**LIGHTHOUSE**  
WORLDWIDE SOLUTIONS

# Facility Monitoring Systems and 21 CFR Part 11 Compliance

by Morgan Polen, VP of Application Technology, Lighthouse Worldwide Solutions  
Dr. Barry Hill – Director, Facility Monitoring Systems

## Introduction

The United States Food and Drug Administration (FDA) is the government agency responsible for the approval of new drugs and the controls for manufacturing of pharmaceuticals consumed in the United States. All drugs manufactured in the United States and all drugs imported to the U.S. are subject to FDA regulations. Different national regulations are similar to the FDA regulations in purpose but the importance of the U.S. market is such that the FDA regulations are given prominence.

The FDA requires all drugs are manufactured in accordance with current Good Manufacturing Practice (GMP) regulations. The pharmaceutical manufacturing company must prove they are in compliance with these regulations at all stages before a drug can be released to the end users. Part of the proof is the collection and storage of data. The collection and storage of manufacturing data is of such fundamental importance that it is not surprising there are many regulations that cover proper record keeping.

Over the past decade, computer systems have become fundamental to the process of collecting manufacturing process data. It to be expected that regulations would be introduced to address the problems inherent in electronic record keeping and the submission of records to the FDA in electronic form. The objective of these FDA regulations is to ensure that data submitted to support any product is trustworthy and can be relied upon.

These regulations were introduced in 1997 as “Electronic Records; Electronic Signatures”<sup>1</sup> commonly known as 21 CFR Part 11 or just 21CFR11<sup>4</sup>.

There have been several FDA guidance documents issued on the application of 21 CFR Part 11, all of which have been superseded in August 2003 by a revised “Guidance for Industry Part 11, Electronic Records; Electronic Signatures Scope and Application”<sup>2</sup>. The revised FDA guidance changed the FDA’s approach to the scope and applicability of 21 CFR Part 11 by basing it on a risk-based assessment for regulatory compliance. This change was to counter the consequences of the original guidance<sup>3</sup>, where producers were adopting strategies that avoided the use of electronic records rather than using computer systems to simplify the collection and reporting of manufacturing information.

Many pharmaceutical manufacturing facilities have automated data collection systems for measuring environmental parameters such as particle counts, pressures, temperatures and humidities. These systems are often known as Facility Monitoring Systems (FMS).

## Facility Monitoring Systems

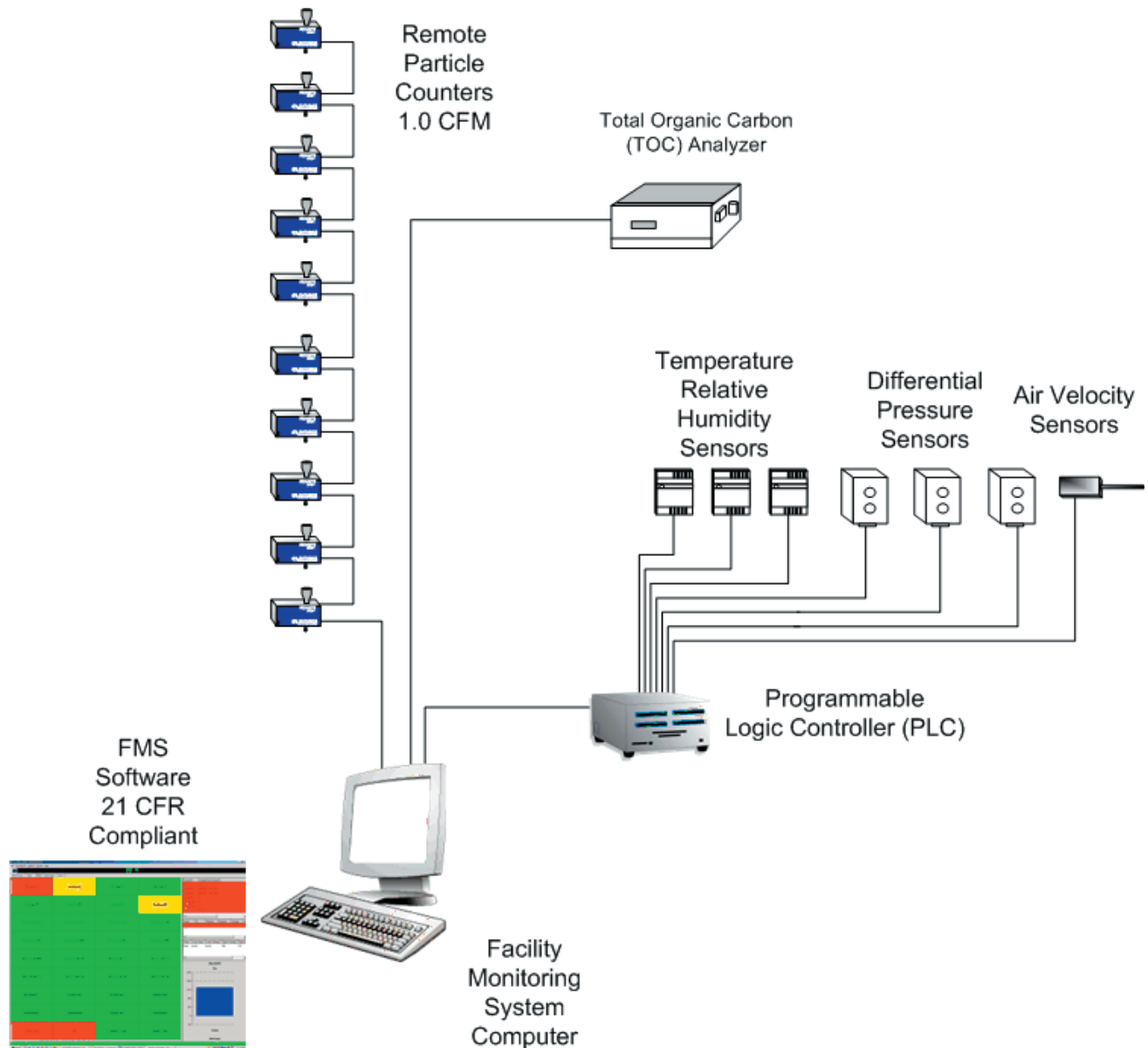
A typical FMS (Fig 1) has a computer that controls inputs from sensors via a network of some description. The data from these sensors is time stamped, stored in a database and displayed. Usually the collected data is compared with alarm limits and, where necessary, alerts are signaled to staff using lights and sounders. An FMS will include reporting facilities. The reports usually include graphs, statistics and tables of collected data. These reports are basic evidence to support a production batch.

FMS installations are, naturally, subject to 21 CFR Part 11.

## Compliance with 21 CFR Part 11

It is not possible for any computer system to be 21 CFR Part 11 compliant *per se*. This is because compliance includes staff, training, physical environment and security, which are all outside the control of any FMS supplier. The end users can only judge compliance, as they are the persons ultimately responsible to the FDA and any other regulatory body.

Figure 1



When a supplier claims “21 CFR Part 11 Compliance” they are usually aware of the problems with such a claim but use it as shorthand for “Providing the necessary facilities to permit an FMS to be made a part of a 21 CFR Part 11 compliant installation”.

Because the end user is the final arbiter in determining compliance with 21 CFR Part 11, this causes problems for suppliers of FMS software. First, there is the question “Is it necessary for a particular facet to be compliant?” and second “What is compliance?” as interpretations may be contradictory and, in some cases, mutually exclusive. The FDA’s “risk-based” approach infers some of the regulations can be considered “optional” but, from an FMS supplier’s point of view, this means compliance with all regulations is required. Any end user may demand, quite properly, that their version of 21 CFR Part 11 is complied with. This is, in effect, no different from the previous guidance where little was optional.

## Security

### Physical Access

Physical access is the first layer of security. It is an unfortunate fact that employees perpetrate malicious acts and data theft from a computer system. Restricting access to a limited number of individuals restricts the physical risk to a system.

Simply locking a computer in a cabinet or office avoids unauthorized access. If you do not have a key, you cannot get access.

## **User Access**

Access to systems requires users to prove they are permitted access, usually by providing a username and a password. Alternatives to usernames and passwords include biometrics and key cards. 21 CFR Part 11 does not specify a particular type of access control, only that a minimum of one biometric or two non-biometric tokens are used.

Usernames and passwords are usually acceptable methods of identification. They are simple and cheap and do not have the problems with biometrics. For example, fingerprint identification is useless if you have to wear gloves.

However, usernames and passwords can be compromised as a result of discovery. Discovery can be watching someone logging in or by hacking usernames and passwords. Social attacks are the most likely: wife's name, cat's name, car registration, etc.

These two threats can be easily countered by incorporating password aging and terminal lockout with an alarm after a small number of failed logins. Password aging forces a user to change the password to a new, different, password at given intervals.

## **Network Access**

Computer systems are often networked to allow users remote access to data. 21 CFR Part 11 defines two types of systems, open and closed. The difference between open and closed systems is a matter of much debate and, as with many things, is a matter of opinion.

A *closed system* is defined as a system in which the owner of the system has complete control over access to the system and its data.

An *open system* is where the owner of the system does not have complete control over access to the system and/or data. An example of an open system is where access is via the Internet. The data, unless encrypted, can be read by a third party and, in principle, modified. If encrypted and secure Internet connections are used then, practically speaking, this cannot happen.

It could be argued that a system that uses encrypted communications is always closed, as any data collected by a third party is useless. In other words, the act of making an open system secure for 21 CFR Part 11 purposes often converts it to a closed system.

Most FMS installations are closed systems. They are responsible for supervising well-defined areas of a plant inside a factory. There is seldom any need to provide access outside the facility, so the system has no reason to be anything but closed.

A networked FMS needs to include access controls that grants access only to other computer systems that have been given permission.

A simple means of controlling access via TCP/IP is by using the network configuration (network mask) that can greatly restrict communications between computers, even if they are wired together.

Wider access can be restricted by using IP addresses that are not recognized across the Internet (such as those starting 192.168), which not only prevent access from outside a facility, but also prevent access to systems outside the local area network (LAN) from within the facility. Although proxy servers can make it possible for any system within a facility to connect to a system anywhere on the internet, this kind of connection can be controlled and, if necessary, prevented by using a network firewall.

## **Audit Trail**

It is important to any 21 CFR Part 11 regime to record when users access a system, when any changes occur to the system and the nature of the changes. This function is called an audit trail.

Normally, these actions must be signed using an electronic signature, described below. The signature links an

action to a responsible individual. In networked systems, the computer being used also needs to be identified.

## **Version Control**

When any configuration is changed, it is necessary to be able to return to an older configuration, if only to determine the nature and effects of the changes.

Version control can take the form of a comprehensive system that allows any combination of previous version to be recovered and tracked, or by simply saving time stamped copies of a configuration.

## **Data Security**

There are two types of data security that are, in part contradictory. One type of data security relates to keeping data secret, the other type of security is keeping the data accessible over long periods of time.

Unless an FMS links collected data to confidential data, such as patient records, the information collected is unlikely to be useful to anyone outside the organization; therefore, the data does not have to be kept secret. However, data must be reliable and alteration must be detectable and reported when found.

The easiest method of data protection is to add a Cyclic Redundancy Check (CRC<sup>6</sup>) to each data record. This can be compared with the original CRC of the data each time the data is retrieved, thus verifying the date. Including record length and position information within the CRC makes alteration without detection nearly impossible.

Encryption also makes alteration very difficult. Encryption works by breaking up data and mixing it with a key. It is very difficult to alter encrypted data because it is turned into (for all intents and purposes) an unintelligible random sequence.

An example of a simple encryption algorithm is given in the online paper, "TEA, a Tiny Encryption Algorithm"<sup>5</sup>. The problem with encryption is that data can only be retrieved if the means of decryption exists. This can cause difficulties over long periods of time.

If a person lives for 80 years, it is possible that data may be needed to investigate the effects of drugs given as an infant on conditions in old age which may be needed, for example, 100 years after the data was collected. Given the rate of obsolescence of computer systems, it is to be expected that the means to read encrypted data may not exist when the data is required. Encryption (and the associated technique of data compression) has the additional drawback that if any data is lost, then all the data is lost.

One way to ensure long term data security is to store the data as plain text. This is more likely to be readable and interpretable over longer periods of time, albeit is at a risk to data confidentiality, should the data be copied improperly.

Ideally, a Facility Monitoring System would offer the facilities to save data using both methods, as well as to achieve generally used databases such as SQL servers.

### *Electronic Signatures*

An electronic signature is a token that is legally the same as an individual's written signature. An electronic signature is not the same as a digital signature. A digital signature is like a checksum added to a file or data record to confirm the source and validity of the file or data packet. An electronic signature can be a user's full name. For example, a user's account name might be jbloggs but his electronic signature could be John X. Bloggs.

To ensure the validity of any electronic signature, it is important that FMS user management ensures that user account names and the associated electronic signatures are unique and are not re-useable. It is also important that the electronic signature is different from the user's account name, as this is half the data required to log on to a FMS.

## References

- <sup>1</sup> 21 CFR Part 11. Electronic Records; Electronic Signatures; Final Rule Electronic Submissions; Establishment of Public Docket; Notice. 21 CFR Part 11 Final Rule
- <sup>2</sup> Guidance for Industry Part 11, Electronic Records; Electronic Signatures; Scope and Application, Final Guidance - August 2003
- <sup>3</sup> Guidance for Industry 21 CFR Part 11; Electronic Records; Electronic Signatures Maintenance of Electronic Records Draft Guidance, July 2002
- <sup>4</sup> The web site [www.21CFRPart11.com](http://www.21CFRPart11.com) is a useful place to start to quickly access 21 CFR Part 11 related documentation. The author does not endorse any products or services promoted by this web site.
- <sup>5</sup> Tiny Encryption Algorithm <http://www.ftp.cl.cam.ac.uk/ftp/papers/djw-rmn/djw-rmn-tea.html>
- <sup>6</sup> T. Ritter, The Great CRC Mystery, Dr. Dobb's Journal, #112, February 1986

## About the Authors

*\*Morgan Polen is Vice President of Applications Technology at Lighthouse Worldwide Solutions, a particle counter systems manufacturer based in San Jose, CA. Lighthouse Worldwide Solutions specializes in facility monitoring systems and components for the Pharmaceutical, Semiconductor, and Disk Drive industries. He can be reached at [mpolen@golighthouse.com](mailto:mpolen@golighthouse.com) or (408) 228-9200. Lighthouse's website is [www.golighthouse.com](http://www.golighthouse.com).*

*\*Dr. Barry Hill is a director of Facility Monitoring Systems Limited (FMS), a supplier of particle counting and environmental monitoring systems and software in the United Kingdom for the Medical, Pharmaceutical and Semiconductor markets. He can be reached at [bhill@fmonsys.com](mailto:bhill@fmonsys.com) or by telephone +44 (0)8702 410862. FMS's web site is [www.fmonsys.com](http://www.fmonsys.com).*

# LIGHTHOUSE



**LIGHTHOUSE**  
WORLDWIDE SOLUTIONS

**46501 Landing Parkway  
Fremont, CA 94538 USA**

**Tel: (510) 438-0500**

**Fax: (510) 438-3840**

**Toll Free: (800) 945-5905**

**Email: [info@golighthouse.com](mailto:info@golighthouse.com)**

**Website: [www.golighthouse.com](http://www.golighthouse.com)**

WORLDWIDE SOLUTIONS