



FDA 21 CFR Part 11

Compliance Guide

Revision F

Overview

According to current good manufacturing practice (CGMP) regulations in parts 210 and 211 of the Code of Federal Regulations (CFR), the U.S. Food and Drug Administration (FDA) requires that strict records be kept during the manufacture and inspection of products manufactured under its control. Originally these records were created and submitted only on paper, but as inspection systems became more computerized, electronic record keeping and submittal became more common.

After accepting comments from human and veterinary pharmaceutical companies, as well as biological products, medical device, and food interest groups, in 1997 the FDA issued the final rule for 21 CFR Part 11 which provides criteria for “acceptance by FDA, under certain circumstances, 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 is divided into three subparts which deal with the scope of the ruling: General (including definitions and implementation), Electronic records, and Electronic signatures. Within subpart B, Electronic records, sections 11.10 and 11.30 define the requirements for closed and open systems. This document addresses how these requirements apply to the Datalogic Automation, Inc. (DLA) machine vision system.

It is important to note that Part 11 states that it is not the equipment manufacturer's sole responsibility to meet the requirements. Those “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 ...” The entire manufacturing, inspection, and record maintenance process must be validated to comply with Part 11.

Datalogic Impact hardware

A DLA machine vision system consists of four different basic configurations, the A-Series Intelligent Camera, the T-series Intelligent Camera, the C-series system, and the M-Series system. The A-Series and the T-series camera are self-contained vision systems which include the camera and processor. The M-Series system consists of a standalone M-Series processor that connects to up to four external cameras. The C-series hardware contains a processor that connects to one external camera. Inspection programs created with the VPM software module reside in the hardware's non-volatile memory.

Impact Software Suite

DLA's vision program development software suite (Impact Software Suite) consists of two main modules, Vision Program Manager (VPM) and Control Panel Manager (CPM). On the A-Series, T-series, and C-series hardware (hosts), these modules run on a personal computer (client) which is networked with them. On the M-Series system, the software modules run on the M-Series processor (client) which is connected through a local network to the cameras.

VPM, which resides in and runs only on the client computer, is used to create and maintain vision programs and provides a panel that allows an operator to view inspection data, and adjust parameters and settings in vision programs. The vision programs reside in and control the A-Series, T-series, C-series, and M-Series hardware. Once a vision program is complete and running on the hardware, VPM is required after that only to make changes to the vision program.

CPM is used to create user-designed control panels which provide a human-machine interface that displays inspection data and allows an operator to adjust parameters and settings in vision programs. Control panels reside in and run only on the client computer. The host to client connection can be one-to-many or many-to-one. That is, a single control panel can connect to multiple hosts and multiple control panels can connect to a single host. Control panels can be configured with User Identification (ID) and password security to limit a user's access to functions on that panel.

The Design and Settings tabs on the VPM module are used by programmers, operators, and supervisory personnel to configure and adjust settings in the machine vision hardware.

An additional module, which resides in and runs only on the client, called CPM Runtime Environment (CPMRE), provides the ability to access the DLA vision system through custom-built control panels. CPMRE provides no capability for editing control panels or vision programs and complies with any program security access built in to the control panel.

Types of Systems under Part 11

Subpart B of Part 11 deals with two types of systems: closed and open. The requirements for each type of system are the same, except that open systems call for "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." The following sections deal with implementing and configuring DLA's vision system to work with each of these two types of systems.

Closed Systems

According to Part 11, a 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."

The following sections briefly describe the requirements of a closed system and how the DLA vision system provides the tools to help customers comply with them.

Section (a) – Validation and the ability to discern invalid or altered records

System validation is the responsibility of the customer. Once the system is validated, strict controlled inspections can be carried out that will confirm the validation process and detect any altered vision program parameters. All of DLA's vision program files are stored in XML format, so altered vision programs can also be detected by comparing the text in an XML file of a running program with the text of a secured backup copy of that file.

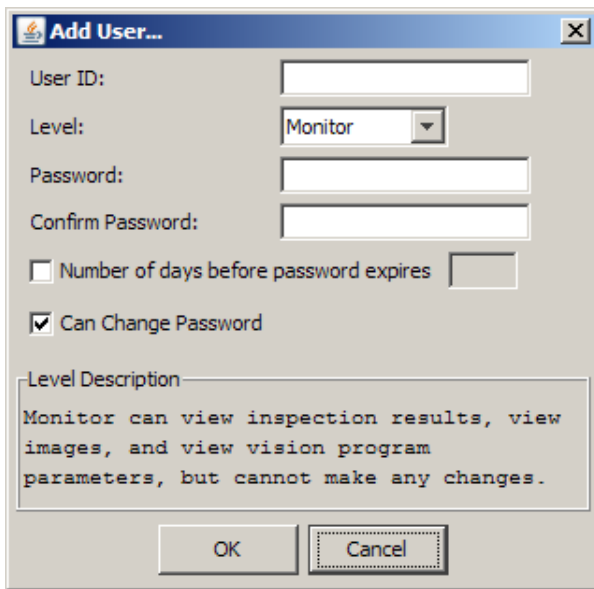
Section (b) – The ability to generate accurate and complete copies of records

Section (c) – Protection of records to enable their accurate and ready retrieval

Each DLA vision device retains a log of system changes and events, in memory, while device power is maintained. This log can be archived, then printed, or copied to a removable storage device on the client computer, and stored in a secure location. The records are protected from unauthorized access by password protection in the vision device.

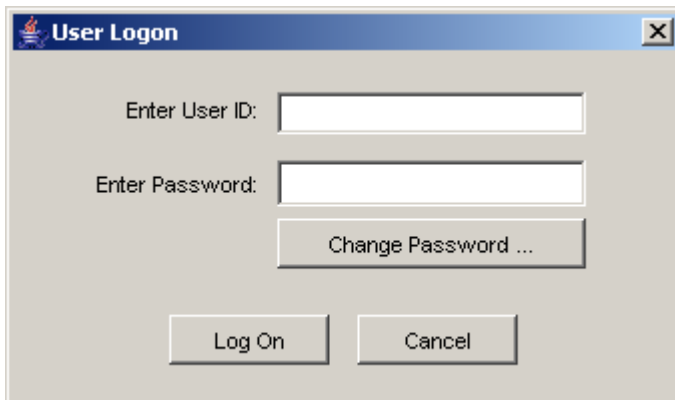
Section (d) – Limiting system access to authorized individuals

Access to DLA hardware devices is controlled by security algorithms that reside on each device. User IDs, passwords, and access levels to the device are defined by system administrators using the Settings tab on the VPM module. Individual vision programs and control panels can be password protected, also.

A screenshot of a Windows-style dialog box titled "Add User...". It contains several input fields and checkboxes. The "User ID:" field is empty. The "Level:" dropdown menu is set to "Monitor". The "Password:" and "Confirm Password:" fields are empty. There are two checkboxes: "Number of days before password expires" (unchecked) and "Can Change Password" (checked). Below these is a text area labeled "Level Description" containing the text: "Monitor can view inspection results, view images, and view vision program parameters, but cannot make any changes." At the bottom are "OK" and "Cancel" buttons.

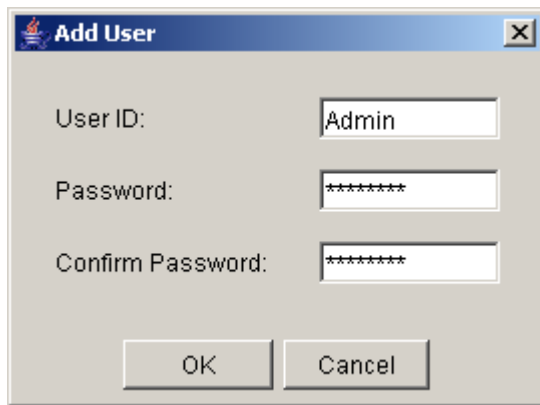
VPM – Defining vision device security access

When anyone attempts to connect to a vision device that has security enabled, they are required to enter a valid User ID and password. The User ID determines the level of access the user has to that device. Vision programs and hardware settings cannot be created, modified, or run without proper authorization.

A screenshot of a Windows-style dialog box titled "User Logon". It contains two input fields: "Enter User ID:" and "Enter Password:", both of which are empty. Below the password field is a button labeled "Change Password ...". At the bottom are "Log On" and "Cancel" buttons.

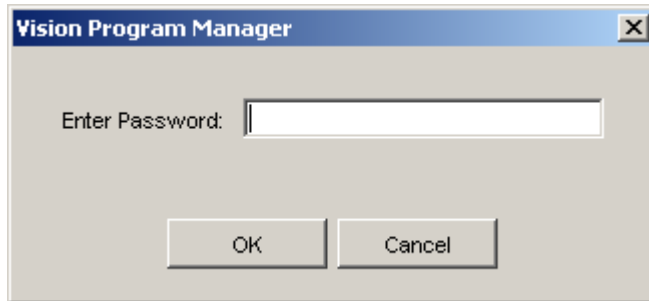
Vision Device Hardware and Control Panel Log On

To protect against unauthorized total access to inspection data or changes to the vision system, password security can be embedded within control panels. This means that, without a User ID and password defined by the control panel creator, a system user cannot view or change inspection parameters on a device even if they have access to that device on the network.



CPM – Defining control panel security access

Even if an unauthorized user gains access to a vision program or control panel outside the DLA vision system, the system provides an additional level of protection at that level. The vision program and control panel can be password protected by the developer to prevent copying them to a different host computer, modifying them, and then copying them back to a DLA vision device.



Accessing a password protected vision program

Section (e) – Use of secure, computer-generated, time-stamped audit trails to independently record operator entries

The DLA hardware provides time-stamped entries in the system log for system events such as operator logon and logoff, vision program loading and unloading, and event triggers. Operator modifications to individual vision program settings (such as tolerances) are not logged. These entries are secure, in that access to the device is password protected. Compliance with this provision can be accomplished by preventing vision program settings changes to the system once validation is complete.

Event	Time
System restarted	Mar 10, 2010 02:15:00:009 PM
Virtual Camera Enabled	Mar 10, 2010 02:15:00:045 PM
Running Impact Version 9.0.0 Build 179	Mar 10, 2010 02:15:01:030 PM
administrator logged on	Mar 10, 2010 02:15:54:821 PM
Vision System Locked by administrator	Mar 10, 2010 02:15:55:506 PM
Unloaded Vision Program "Inspection"	Mar 10, 2010 02:18:53:332 PM
1, 1, AppClosedEvent	Mar 10, 2010 02:18:53:346 PM
Loaded Vision Program "Inspection" from file /cf/VisionPrograms/passwordis...	Mar 10, 2010 02:18:58:677 PM
3, 1, AppOpenedEvent	Mar 10, 2010 02:18:58:677 PM
Unloaded Vision Program "Inspection"	Mar 10, 2010 02:19:22:648 PM
5, 2, AppClosedEvent	Mar 10, 2010 02:19:22:649 PM
Time before clock was set.	Mar 10, 2010 02:22:07:843 PM
Time after clock was set.	Mar 10, 2010 02:22:07:843 PM

System Log example

Section (f) – Use of operational system checks

This is the customer's responsibility.

Section (g) – Use of authority checks to ensure that only authorized individuals can use the system

It is the responsibility of the customer to perform authority checks and prevent unauthorized access to the system.

Section (h) – Use of device checks to determine the validity of the source of data input

In addition to the Impact password security mentioned in Section (d) above, DLA vision programs can be prevented from running on a vision device. The vision program creator can check the serial number of a vision device and prevent the program from running on that device if the serial number does not match. This ensures that the program runs only the device for which it intended.

Section (I) – Determination that persons who develop, maintain, or use the systems have education, training, and experience

This is the customer's responsibility.

Section (j) – The establishment of, and adherence to, written policies

This is the customer's responsibility.

Section (k) – Use of appropriate controls over systems documentation

This is the customer's responsibility.

Open Systems

According to Part 11, an Open system means “an environment in which system access is not controlled by persons who are responsible for the content of records that are on the system.”

The additional requirements for open systems, including “document encryption and use of appropriate digital signature standards to ensure record authenticity, integrity, and confidentiality” exceed the capabilities of the DLA hardware and software. DLA recommends using 3rd party software that provides the necessary capabilities. Many Supervisory Control and Data Acquisition (SCADA) systems on the market provide secure, encrypted database logging and can be configured to fulfill all the requirements of this section. Another advantage of using this configuration is the ability to control multiple supervisory control devices, including the DLA hardware, from a single, centralized control system.

Impact Software Suite provides multiple communication tools to help integrate vision programs on the DLA hardware with control panels running on a SCADA system. Serial and Ethernet connections are standard on the vision systems. Ethernet data transfer can use HTTP or TCP/IP protocol. Impact Software Suite software also provides tools to transfer data between DLA and other industry standard Ethernet/IP devices.