

Cognex In-Sight® Vision Sensors 21 CFR Part 11 Application Guidelines

This document is intended to be a guide, and is not to be relied upon for compliance purposes. Additionally, federal regulations often change; these guidelines are current as of the date indicated in the page footers. Per FDA, the regulated customer is responsible for knowing the current version of these regulations and complying with all aspects of these, and any other, applicable federal regulations.

Cognex In-Sight Vision Sensors 21 CFR Part 11 Application Guidelines

OVERVIEW

Founded in 1981, Cognex® set out to develop computer-based systems that could “see.” Today, our machine vision systems are used around the world to accurately gauge, guide, identify, and inspect products — at up to thousands of parts per minute, and in virtually all industries. Proven Cognex technology has provided customers with greatly improved productivity and quality, as well as lower manufacturing costs. With more than 200,000 vision systems sold, over 35 percent of employees engineers, and a technical support organization that spans the globe, Cognex has become the world’s leading supplier of machine vision systems.

Our vision systems and sensors are used throughout pharmaceutical manufacturing. Manufacturers in the pharmaceutical industry are turning to Cognex machine vision to help reduce product defect rates and increase line efficiency. This industry relies on Cognex systems to check date and lot codes, read bar codes, inspect packaging, and confirm that bottles are correctly labeled, capped, and sealed.

The 21 CFR Part 11 rule, enacted in 1997, provides criteria for compliance of all regulated electronic records systems, and provides guidelines for product safety and traceability in electronic records and control systems in pharmaceutical and other industries. The key areas addressed by the rule are data security, data integrity, audit trails, and signature authority.

Manufacturers and suppliers have been dealing with the interpretations and impacts of this rule for the last several years, leading Cognex to take a proactive approach to interpret what FDA Part 11 compliance means from a vision system supplier’s point of view. We have taken several significant steps to assist our customers in their compliance efforts, now and in the future. For example, Cognex has taken a step-by-step gap analysis to determine how our products may be applied to support 21 CFR Part 11 when integrated and implemented properly with Cognex products’ standard features and complementary technologies.

IN-SIGHT 1000/3000/4000/5000 VISION SENSORS AND THE 21 CFR PART 11 REGULATION

This section describes the application of the In-Sight® 1000, 3000, 4000 and 5000 Series vision sensors under the 21 CFR Part 11 regulation, highlighting the following areas:

- Security and safeguards
- Computer-generated time-stamped audit trails
- Signature/record linking
- Validation

In this document, all references to “In-Sight vision sensors” or to “In-Sight units” refer solely to the In-Sight 1000, 3000, 4000 and 5000 Series.

Security and Safeguards

Each In-Sight vision sensor is equipped with built-in Ethernet communications, allowing multiple In-Sight units and PCs to be easily linked together. Therefore, procedural measures are required to control operator access to the hardware systems. In the networked client-server environment, for example, it is recommended that the end-user utilize only one PC server to operate and control the entire network (closed system) in order to control access. Furthermore, for enhanced security, several vendors offer desktop products with controlled access via a locking feature.

The In-Sight PC Host program in the Microsoft® Windows NT®/2000/XP operating system domain can use the username and password security mechanisms built into Windows NT®/2000/XP. Several third-party security software solutions exist for extended security protection, such as re-authentication.

In addition to PC security access, each In-Sight unit on the network provides three levels of access with username and password protection. The end user can create a unique application to interface with networked In-Sight units that includes username and password protection via Telnet and Native Mode communications.

The automatic synchronization of usernames and passwords between PC Host and In-Sight vision sensors can be accomplished using a front-end programming language, such as Visual Basic. By default, In-Sight vision sensors are configured to automatically receive unique IP Address and Subnet Mask settings from a DHCP server when connected to network. (More information about New Host Configuration Dialog is available in the In-Sight Guide and Reference, under this topic.)

Password aging can be enforced by Windows NT/2000/XP network access security. For extended security protection Cognex recommends the use of third-party security software for Windows NT 4.0, 2000 and XP.

Windows NT/2000/XP security mechanisms can detect unauthorized use if rules for unauthorized use are defined and maintained. (For example, a rule might specify that three incorrect log-in attempt generates a suspension of the account.) Nevertheless, end-user customers should put policies and procedures in place to prevent unauthorized users from accessing the system.

Computer-generated time-stamped audit trails

Under the NT domain, the PC Host should be configured by the regulated customer to automatically generate records with time, date, and an electronic signature of the logged-in operator.

Signature/record linking

The end-user should store all job and event files in a protected database. All data records stored in a relational database (e.g. SQL Server or Oracle) should be protected by a username and password, preventing information from being altered by unauthorized persons.

Validation

The regulated customer must validate applications. Customers may develop and execute validation plans and protocols themselves or outsource these activities to independent, qualified companies. Cognex provides relevant hardware specifications with user documentation to help customers expedite the validation process.

To further comply with data source validity, it is recommended that the regulated customer use third-party version control software, such as Microsoft SourceSafe, to maintain job and event files, databases, and I/O configurations. The version control software should be accompanied by a set of procedures and policies on conventions and use.

COMPLIANCE SUMMARY

21 CFR Part 11 Section Number	Requirement	In-Sight 1000, 3000, 4000 and 5000 Vision Sensors
B11.10	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:	The regulated customer should develop procedures to support the use of the vision applications in a regulated environment.
B-11.10.a	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	The regulated customer must validate the applications. Customer may develop and execute the validation plans and protocols themselves or outsource these activities to independent qualified companies. Cognex provides relevant hardware specifications, with user documentation, to help the customer expedite the validation process.
B-11.10.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.	Job configuration setups and historical alarm records should be maintained in a third-party relational database and can be retrieved/printed through a variety of third-party data retrieval tools.
B-11.10.c	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	A relational database can be configured for security. The regulated customer should put procedures in place to ensure that records are retained for an appropriate duration of time.
B-11.10.d	Limiting system access to authorized individuals.	Standard procedures to limit physical access are the responsibility of the regulated customer. In-Sight 1000/3000/4000/5000 and Windows security are utilized to limit user access to assigned functionality. In-Sight provides 3 levels of access with username and password protection.

21 CFR Part 11 Section Number	Requirement	In-Sight 1000, 3000, 4000 and 5000 Vision Sensors
B-11.10.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.	The regulated customer should ensure that job setups and historical alarm records cannot be altered. All audit trail records should include date and time stamp, node of origination, and username. The regulated customer should implement a Windows or third-party clock synchronization utility to create an action log for each entry activity and to ensure that all date and time stamps are accurately recorded in the audit trail.
B-11.10.f	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	The regulated customer can build systems that implement a combination of In-Sight and NT/2000/XP security that support the use of operational checks.
B-11.10.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.	Both In-Sight and Windows security may be utilized to limit user access to assigned functionality. In-Sight security may be utilized to limit user access to sensor level functionality while Windows security may be utilized to limit operator access to the PC workstation.
B-11.10.h	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	To ensure the validity of the source of data input, the regulated customer should use a single PC server to manage and control the networked In-Sight units. All records should be stored to the server computer only. In-Sight security may be utilized to limit user access to assigned functionality.
B-11.10.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.	The regulated customer is responsible for ensuring that all individuals who develop, maintain, or use the systems are properly educated to perform their task.
B-11.10.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.	The regulated customer is responsible to ensure that the policies and procedures are in place to support the use of vision applications in a regulated environment.

21 CFR Part 11 Section Number	Requirement	In-Sight 1000, 3000, 4000 and 5000 Vision Sensors
B-11.10.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.	Cognex provides <i>In-Sight Guide & Reference</i> manuals to its customers upon purchase. The document is provided on a CD-ROM and secured web site in read-only format. It cannot be modified by the customer. Although end-user customers are not responsible for control over the content of In-Sight Guide & Reference manuals, they should establish and maintain controls over the distribution of, access to, and use of that documentation.
	2. Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Source files for Cognex manuals are version-controlled documents, and a history of all revisions is maintained.
B-11.50	SIGNATURE MANIFESTATIONS	
B-11.50.a	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:	The regulated customer is responsible for incorporating the following items into signed electronic records. This functionality must be provided outside the In-Sight vision sensor, and outside the PC Host operating environment.
	1. The printed name of the signer	The username of the operator is logged to the records along with all events.
	2. The date and time when the signature was executed.	The date and time is logged to the records along with all events.
	3. The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	The activity type to which the event is tied is logged to the records along with all events.
B-11.50.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 items identified in paragraphs (a)(1), (a)(2), and (a)(3) are stored in the same databases as mentioned in the above sections and therefore are subject to the same controls as for electronic records.

21 CFR Part 11 Section Number	Requirement	In-Sight 1000, 3000, 4000 and 5000 Vision Sensors
B-11.70	SIGNATURE/RECORD LINKING Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	The regulated customer should ensure that each audit trail record includes the name of the user linked to the specific activity. The event records are maintained in a third-party or customer provided relational database, and utilize an audit trail to prevent falsification. The regulated customer should also establish policies and procedures to prevent unauthorized access to the database containing the audit trail file.
C-11.100	GENERAL REQUIREMENTS	
C-11.100.a	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	In-Sight 1000/3000/4000/5000 and Windows security require that all username and password combinations are unique. The regulated customer is responsible for ensuring that electronic signatures are unique to one individual and not reused by any other individual.
C-11.100.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.	It is the responsibility of the regulated customer to verify the identity of all individuals who will utilize the system.
C-11.100.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.	It is the responsibility of the regulated customer to 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.	It is the responsibility of the regulated customer to submit the certification to the Office of Regional Operations.
	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.	It is the responsibility of the regulated customer to 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.

21 CFR Part 11 Section Number	Requirement	In-Sight 1000, 3000, 4000 and 5000 Vision Sensors
C-11.200	ELECTRONIC SIGNATURE COMPONENTS AND CONTROLS	
C-11.200.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.	In-Sight should be configured to use Windows NT/2000/XP security, which employs a user ID and password to identify a user.
	1. (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.	Windows security requires the user to enter their username and password to gain access to the system. For creating a re-authentication environment, Cognex recommends the use of third-party security software solutions for Windows NT 4.0, 2000 and XP.
	1. (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.	For creating a re-authentication environment, Cognex recommends the use of third-party security software solutions for Windows NT 4.0, 2000 and XP. The regulated customer should also implement policies and procedures requiring users to log out of the application during periods of non-use.
	2. Be used only by their genuine owners	It is the responsibility of the regulated customer to put policies and procedures in place that ensure that the electronic signatures are only used by their genuine owners.
	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.	The regulated customer should have procedures in place to force users to change their passwords after being initially set by the administrator. This functionality is supported by Windows security — "User must Change Password at Next Logon" function.
C-11.200.b	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners	This is the responsibility of the regulated customer in the selection of biometrics based mechanism to be used with the system.

21 CFR Part 11 Section Number	Requirement	In-Sight 1000, 3000, 4000 and 5000 Vision Sensors
C-11.300	CONTROLS FOR IDENTIFICATION CODES AND 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:	
C-11.300.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.	In-Sight should be configured to use Windows NT/2000/XP security, which centrally requires that all username and password combinations are unique.
C-11.300.b	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	In-Sight should be configured to use third-party Windows NT/2000/XP security software, which can be configured to enforce password aging.
C-11.300.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.	The regulated customer should implement 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-11.300.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.	Windows security can be configured to disable a users account after consecutive failed logons.
C-11.300.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.	The regulated customer should perform initial and periodic testing of devices to ensure that they function properly and have not been altered in an unauthorized manner.

Appendix

Networked Vision Sensor Integration Considerations

Data Exchange, Remote Control, and Security Management

Introduction and Purpose of This Document

This Appendix is intended for use by customers that wish to learn more about the many options available for integrating a networked In-Sight vision sensor into an automated production line. The emphasis is on the use of standard open systems networking protocols to achieve the required functionality and performance in the least amount of time. This document assumes that the user is already familiar with the In-Sight spreadsheet development environment and its network I/O functions, as well as the Native Mode command set. Please refer to In-Sight online help for details on these topics. A companion demonstration program in the Microsoft Visual Basic® development system is available to illustrate use of the technologies described in this Appendix.

Overview of Integration Considerations

For each application, users first must consider their exact requirements for vision sensor integration. For example, will remote control of the sensor be required, or will capture of individual vision result data be sufficient? If remote control is necessary, will it be achieved via an Ethernet network connection, or by non-network methods such as discrete and serial I/O? In-Sight also offers multiple levels of user access security, which can be remotely updated. This document describes the options available for network integration and illustrates some specific examples:

- **Exchanging Data With Networked In-Sight Systems**

Data Exchange with networked In-Sight vision sensors is most often achieved by using the standard Transmission Control Protocol/Internet Protocol (TCP/IP) connection over the ethernet. The use of the Microsoft Winsock TCP/IP socket control for exchange of plain text data with the In-Sight sensor will be illustrated. Automated file transfers via the Microsoft Internet Transfer Control will also be described. In the content of networked In-Sight sensors, these files contain job, image, and I/O setting information.

- **Remote Control of the In-Sight Vision Sensor**

The In-Sight “Native Mode” command set is provided for remote control of the vision sensor over Ethernet networks. Before employing Native Mode, the user establishes a standard Telnet remote logon to the vision sensor, and then issues simple commands to perform functions such as retrieving current job name, or going online or offline.

- **User Access and Security Considerations**

In-Sight provides multi-level user access, including logon names and passwords that are under control of the sensor administrator. Many users choose to extend In-Sight security; for example, to handle logoff after user inactivity, and timestamped logon/logoff tracking. Cognex recommends the use of third-party security software solutions for Windows NT 4.0, 2000 and XP to achieve this extended security protection.

Overview of a Generic Networked Vision Application Program

In our example, a simple Visual Basic user interface (UI) is constructed using standard software controls from Microsoft. This UI provides several services, including sensor security management, data exchange, image retrieval, image archiving, remote command issue, and command response handling. Image data is stored locally on the PC hard drive in bitmap format, while individual vision sensor result data is stored (and graphed) in MS Excel spreadsheets. The Visual Basic application establishes bidirectional communication with the sensor via Telnet/Native Mode (or TCP/IP, using the MS Winsock control) and FTP (using the MS Internet Transfer Control). It communicates to Excel by use of standard OLE automation.

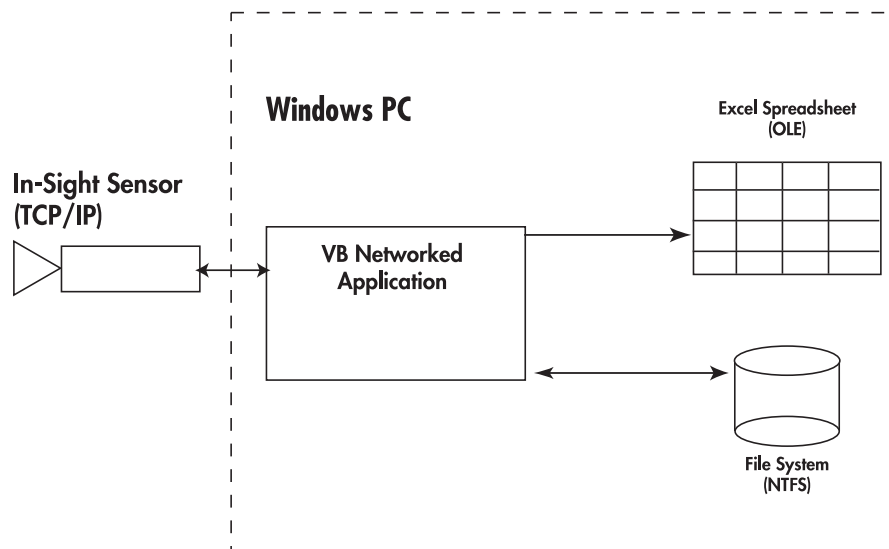


Figure 1: Block Diagram of an Integrated Vision System using the Windows PC platform

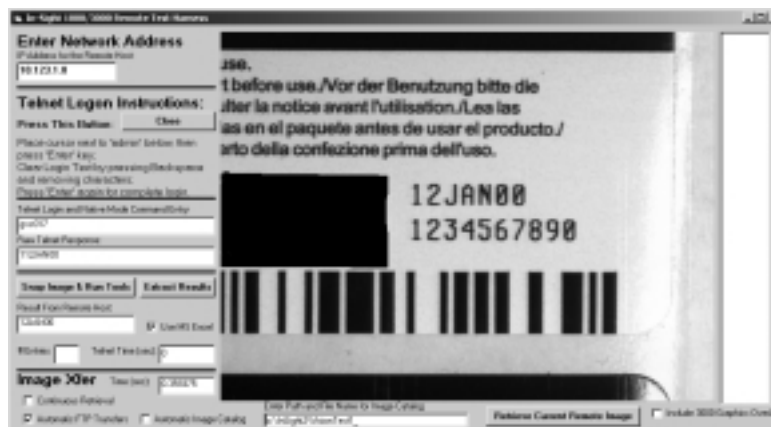


Figure 2: Sample Windows PC Network Application created in Visual Basic

The Details of Data Exchange

Data Exchange can be broken down into two areas: individual data (such as vision system results) and larger blocks of data (such as image files). Exchange of smaller, individual pieces of data is covered in this section, while file transfer is addressed in a later section.

Telnet (NM Communications)

It is very easy to quickly read (or write) data from (or to) any In-Sight spreadsheet cell. The details of Telnet/Native Mode operation are covered first. The user must logon to the In-Sight system on port 23 by inputting a correct user ID and password combination.

The complete list of Native Mode commands can be found in the In-Sight HTML help file. As an example, the Native Mode command used to read data is GV ("Get Value"), followed by the spreadsheet cell location. In order to retrieve the string result from cell E2, the Native Mode command format is "GVE002". Each Native Mode command contains, at a minimum, a return value that indicates one or more return values that indicate the status of the last requested transaction, which is helpful in establishing methods for error handling and command retries.

TCP/IP Client/Server Communications

Optionally, users may wish to use an asynchronous data exchange method based on pure TCP/IP packet transfers. In this case, the TCP Device function(s) must be pre-defined in the spreadsheet of the target sensor. If the device is acting as a client, then both remote IP address and port number must be supplied. Once the connection is established, the incoming data will be updated as it arrives at the sensor, while outgoing sensor data is dependent on a user-specified event.

Modbus/TCP Communications

The Modbus/TCP protocol is also available as the data exchange method. In this case one device would act as server on port 502, while the other would initiate communication of packets whose contents are organized according to the Modbus/TCP specification.

Even more data transfer protocols will be added to In-Sight in the future. Regardless of the method used for transfer, the data retrieved to the PC from the In-Sight sensor can then be integrated or directed to any number of PC-based applications. In our example, we record the result from each vision operation in an Excel spreadsheet. It would be just as easy to place this data into an Access database, or any 32-bit Windows application that supports OLE (or DDE).

The Details of Remote Control

The Details of File Transfer and Archiving

The standard FTP protocol is used when sending or retrieving files to or from the In-Sight unit. These files can be vision jobs, images acquired on the sensor, or sensor settings files. In the case of vision jobs, users will often store these files in a central networked location in order to provide quick distribution to any sensor location on the factory floor.

In the case of image files, users have the option to archive the current image to a central storage location. This provides the ability to perform off-line analysis of a part that was failed by the vision system, or to simply get a quick look at how parts currently appear. In our example program, the files can be archived automatically by incrementing a filename. Alternatively, a user-provided timestamp could be written as part of the file name, or even as part of the image data itself. If an SNTP (Simple Network Time Protocol) is available, networked In-Sight sensors can be configured to send date and time stamp information.

The last file type that applies to use of the In-Sight vision sensor is the settings file. This file contains the current I/O and startup configurations and user list for security. This file is created and maintained by use of the In-Sight PC Host software program, which is distributed with In-Sight model 1000, 3000, 4000 and 5000 vision sensors. By default, only users with administrative privileges can change the contents of a settings file. Since the file contains security information, the portion containing the login profiles is encrypted, while other parts of the file are human readable. Once a settings file is sent to a remote sensor, that sensor immediately adopts the I/O and security settings specified in the file. This means that settings can be stored in a central network location and quickly distributed to sensors in remote locations on the factory floor. As new operators and supervisors are added to the staff at the factory or as passwords need to be changed, updated sensor settings files can be distributed automatically over the network.

The Details of Sensor-Level Security in a Windows Environment

Continuing with our discussion of Native Mode commands via Telnet logon, we move now to applying this interface for the purposes of remotely controlling the operation of the vision sensor. Although most sensors will acquire their next image based on a hardware trigger from the factory floor equipment, it is also possible to place the acquisition event under software control. In this case, the Native Mode command is called "Set Event", and event 8 is tied to image acquisition. Therefore, as long as the sensor is online with a TelNet connection, we would simply issue the string "SE8" to trigger the sensor.

However, in most cases, remote control goes beyond image acquisition. For instance, it is also possible to toggle the Online/Offline status of the vision sensor, query the name of the active vision job, and load a new vision job from local sensor memory as part of a production line changeover process. These operations rely on the use of In-Sight's Native Mode command set, which is documented in detail in the online help file that comes on the CD software distribution.

As stated earlier, networked In-Sight products provide multi-level access security through a settings file that is stored locally on each sensor. As long as this manually configured settings file contains the latest logon security information, it can be shared to any sensor or group of sensors.

Certain users may wish to go beyond having access security at the sensor level. For instance, a restriction on "idle time after login" may be required. In this case, the use of third-party security controls for Windows is required. Some popular vendors and resources are listed below, by web address:

<http://www.bardon.com/>

<http://www.pedestalsoftware.com/>

<http://www.sans.org/newlook/publications/ntstep.htm>

Refer to www.microsoft.com for more information regarding Windows NT security.

Using Sample Code To Help Get You Started

Our Visual Basic example is available to help illustrate the details of networked vision sensor integration. Even if you are not planning to implement your solution in VB, this code is well-commented and can be a valuable planning aid. The demo program expects to retrieve a string from a single spreadsheet cell.

- Step 1: Launch the In-Sight PC Host program "In-Sight.exe", as well as the demo program "NetBenchDemo.exe"
- Step 2: In the demo program, enter the IP address of the In-Sight sensor and follow the provided logon instructions
- Step 3: After receiving the message "User Logged On", enter your Native Mode command
(Example command: "GVC017" to get the value in spreadsheet cell C17)
- Step 4: With sensor online and configured for manual or external acquisition trigger, press the "Snap Image" button
(Press the "Retrieve Image" button to get a bitmap copy of the image on the local PC hard drive)
- Step 5: Press the "Extract Results" button to run the Native Mode command and copy result to Excel
- Step 6: Place a new part or reposition existing part under the In-Sight camera and repeat steps 4 and 5

NOTE: The demo is currently configured to retrieve and transfer string data results only. See code comments on how to retrieve numeric values instead.

COGNEX

Vision for Industry®

Corporate Headquarters
Cognex Corporation
One Vision Drive
Natick
MA 01760-2059
USA
Tel: (508) 650-3000
Fax: (508) 650-3344
www.cognex.com

Primary Sales Offices

United States	www.cognex.com
Eastern Region	(508) 652-3880
Natick, Massachusetts	
Southern Region	(615) 844-6158
Nashville, Tennessee	
Central Region	(248) 668-5100
Detroit, Michigan	
Midwest Region	(630) 649-6300
Chicago, Illinois	
Western Region	(650) 969-4812
Mountain View, California	

Europe	www.cognex.net
France	+33 1 4777 1550
Germany	+49 721 6639 0
Ireland	+353 1 825 4420
Italy	+39 02 6747 1200
Netherlands	+31 402 668 565
Sweden	+46 21 14 55 88
Switzerland	+41 71 760 05 57
United Kingdom	+44 1908 206 000

Canada	www.cognex.com
	(905) 634-2726
Japan	www.cognex.co.jp
	+81 3 5977 5400
Southeast Asia	www.cognex.net
China	+86 21 6407 5835
Korea	+82 2 539 9047
Singapore	+65 6325 5700
Taiwan	+886 3 562 6660

