IT Security for Industrial Control Systems: Requirements Specification and Performance Testing

Presented at the 2004 NDIA Homeland Security Symposium & Exhibition
Hyatt Regency, Crystal City, Virginia, May 25-27, 2004

Joseph Falco, James Gilsinn, Keith Stouffer
Intelligent Systems Division
National Institute of Standards and Technology (NIST)
Gaithersburg, MD

Email: (joseph.falco@nist.gov, james.gilsinn@nist.gov, keith.stouffer@nist.gov)

ABSTRACT

The United States Government as well as the industrial controls sector has come to realize that securing computer systems that control industrial production and distribution is vital to the protection of key components of its critical infrastructure and the health of the associated economies at risk. Current systems are designed first and foremost to meet performance, reliability, safety, and flexibility requirements. Yet, as these systems are steadily integrated with information technology (IT) solutions to promote corporate connectivity and remote access capabilities, serious new vulnerabilities are being introduced into the operational system components. To address these issues, the National Institute of Standards and Technology (NIST) is defining and applying standard information security requirements for information security products and approaches to secure industrial control systems. NIST is also developing performance test methods to insure that resultant security solutions do not adversely affect the critical operational requirements of these control systems.

The NIST work to define security requirements for industrial control systems is being carried out by the Process Control Security Requirements Forum (PCSRF). The PCSRF is a NIST mediated working group of representatives from various industrial sectors and vendors that design, produce, and/or integrate components and systems for the industry. The group is also supported by professional and governmental organizations. The PCSRF is working with security professionals to assess the vulnerabilities and establish appropriate strategies for the development of policies and countermeasures that the U.S. industrial controls community would employ through a combination of IT and non-IT mechanisms to reduce residual risk on its control systems to an acceptable level. The Common Criteria for Information Technology Security Evaluation, also known as ISO/IEC 15408, is being used to document the results of this effort in the form of Protection Profile security specifications.

Parallel to the PCSRF efforts, NIST has developed a laboratory scale testbed comprised of several implementations of typical industrial control and networking equipment as well as relevant sensors and actuators. This testbed is being used to develop performance metrics and tests that can be applied to industrial control security products to determine if particular time-sensitive requirements can be met. These performance metrics pertain to real-time requirements for data transfer, such as minimal latency and timing jitter, and are not considered in traditional IT networks. Work being performed on this testbed includes the development of metrics and tests to evaluate the performance of industrial networking equipment as well as the development of tests for evaluating the effects of security implementations on the operation of industrial control systems.

Commercial equipment and materials are identified in order to adequately specify certain systems. In no case does such identification imply recommendation of endorsement by the National Institute of Standards and Technology, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

Products undergo testing to determine the validity of the testing procedures and the range of results that can be expected with commercial systems. Any results will be reported either in aggregate, or with any vendor-identifying information removed.

INTRODUCTION

The computer systems that control industrial production and distribution have been designed first and foremost to meet performance, reliability, safety, and flexibility requirements. Yet these systems increasingly incorporate connectivity and remote access capabilities. Industry is becoming aware that increased connectivity and openness are introducing serious new vulnerabilities into their operational systems. In addition, the US Government has come to realize that securing these same systems is vital to the protection of key components of its critical infrastructure [1]. There are many risks associated with information technology (IT) threats to industrial control systems. The most consequential risks, those associated with the health and safety of human lives, primarily belong to industries defined as part of the US Critical Infrastructure. Cyber attacks on industrial production and distribution systems, including electric, oil, and gas, water treatment and distribution systems, as well as on chemical plants containing potentially hazardous substances could endanger public health and safety as well as invoke serious damage to the environment. Attacks on any industrial control system could also result in serious financial implications including loss of production, generation or distribution of a product, or compromise of proprietary information and creation of liability issues.

To help US industry address these issues, the National Institute of Standards and Technology (NIST) has initiated an industry wide group called the Process Controls Security Requirements Forum (PCSRF). The PCSRF is a working group that includes representatives from various industrial sectors and vendors that design, produce, and/or integrate components and systems for the industry, professional organizations, government organizations and security professionals. The goal of this group is to assess vulnerabilities and to design and document a set of security specifications using the Common Criteria for Information Technology Security Evaluation, also known as ISO/IEC 15408. Now in its 3rd year, the PCSRF has produced a Security Capabilities Profile (SCP) document and a System Protection Profile for Industrial Control Systems (SPP-ICS) document. The SCP document serves as a means to reach consensus within and across the various industries regarding the security capabilities that are required in a secure industrial control system. The SPP-ICS is a baseline system level protection profile, which defines an integrated set of security requirements for the entire system lifecycle. This SPP-ICS serves as a starting point for more specific system protection profiles such as a Distributed Control System (DCS) or a Supervisory Control and Data Acquisition (SCADA) system, for a specific instance of an industrial control system, and for component protection profiles such as an industrial controller or sensor authentication.

Real-time computer control systems used in industrial control applications have many characteristics that are different from traditional information processing systems used in business applications. Foremost among these is design for efficiency and time-critical response. A generic diagram of the components within a typical industrial control system is shown in Figure 1 [2]. Measurement variables are transmitted to the controller from the process sensors. The controller interprets the signals and generates corresponding control signals that it transmits to the process actuators. Process changes result in new sensor signals, identifying the state of the process, to again be transmitted to the controller. The Human Machine Interface (HMI) allows a control engineer or operator to configure set points, control algorithms and parameters in the controller. The HMI also provides displays of process status information, including alarms and other means of notifying the operator of malfunctions. Diagnostic and maintenance tools, often made available via modem and Internet enabled interfaces, allow control engineers, operators and vendors to monitor and change controller, actuator, and sensor properties from remote locations. A typical industrial system contains a proliferation of control loops, HMIs and remote diagnostics and maintenance tools built on an array of network protocols. Supervisory level loops and lower level loops operate continuously over the duration of a process at cycle times ranging on the order of minutes to milliseconds.

Security in these systems is generally not a strong design driver and therefore has tended to be bypassed in favor of performance. Computing resources (including CPU time and memory) available to perform security functions tend to be very limited, since in most cases security is being implemented as an afterthought. Furthermore, the goals of safety and security sometimes conflict in the design and operation of control systems. Industrial control networks have real-time requirements that may be disrupted by existing security technology such as firewalls. NIST is addressing these issues though the development of performance metrics and tests for industrial control system security implementations to ensure that time sensitive data transfer requirements can be met.

This paper first describes the efforts and progress of PCSRF to address security requirements for industrial control systems and components. An industrial control systems security testbed that has been developed at NIST is then described. Current testbed activities are then presented. These include the development of performance measures of control system execution when security solutions are introduced, and the development of performance metrics and tests for industrial Ethernet devices.

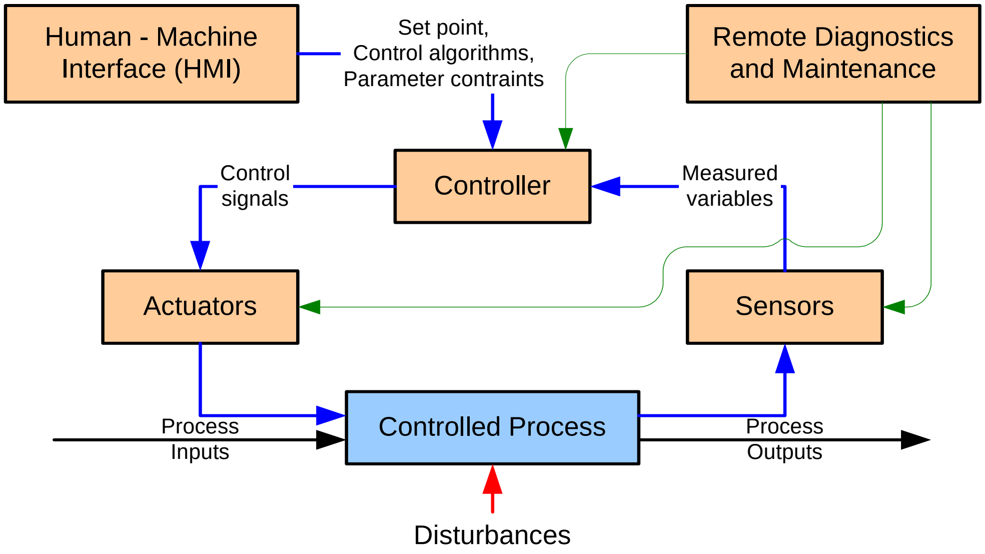

Figure 1 - Generic Industrial Control System

PCSRF SECURITY REQUIREMENTS DEFINITION

The PCSRF [3] addresses the cyber security requirements for industrial control systems and components, including DCS, SCADA systems, Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), and Intelligent Electronic Devices (IEDs) – microprocessor-based protective relays. The main goal of the PCSRF is to increase the security of industrial control systems through the definition and application of a common set of information security requirements for these systems. This will reduce the likelihood of successful cyber-attack on the nation’s critical infrastructures.

A Common Criteria Based Approach

The PCSRF is developing its security specifications using the Common Criteria (CC). The CC, ISO/IEC 15408 [4], is a meta-standard of criteria and constructs used to develop security specifications in support of the evaluation of products and systems. The specifications define and characterize the security problem including assumptions about the operational environment, threats that may be encountered and policies that must be enforced. Also characterized is the intended approach to eliminate, minimize or monitor defined threats, and enforce stated policy. The specification defines functional requirements, specifying what the system is to do and assurance requirements, specifying what is done to verify that the system does exactly what it is supposed to. These CC requirements, selected from a catalog of criteria, are independent of technology and implementation. The finished specification is a formal CC Protection Profile (PP) for a product or system. A PP is applied to serve as an acquisition/procurement vehicle to specify the security requirements of a component or system design or to gauge the security features of available components or systems. A PP can also be applied to verify product compliance both at the component evaluation level and at the system certification level.

Security Capabilities Profile (SCP) Document

The PCSRF has developed the Security Capabilities Profile (SCP) [5] as a first step towards development of PPs for industrial control systems. The SCP is a document used to reach consensus within and across the various industries regarding the security capabilities that are required to secure an industrial control system. To develop this document, industry specific working groups were formed to define vulnerabilities specific to their industrial control system based on a set of system functions and capabilities defined by the PCSRF. The results of the individual vulnerability assessments were analyzed and consolidated, by the PCSRF and Decisive Analytics, a security consultant, into comprehensive statements of vulnerabilities that are listed in the SCP document. The document defines a superset of security capabilities that would exist in electronic programmable components that comprise an industrial control system. Each operational Industrial Control System (ICS) will need to apply these capabilities as appropriate for that system's environment. The security and safety risks of the operational environment of the ICS must be assessed for each ICS. Based upon the security and safety environment in which the ICS components must operate, individual security capabilities will be specified, configured, and employed by customers to meet the overall security needs of the ICS. The specific configuration of the components to support organizational security and safety objectives is left to the system designers to implement. For each selected capability, the specific requirements statements should be reviewed and modified to provide the desired level of functionality and assurance. The document also serves as a vehicle to convey to the industrial control system and component vendors the security capabilities that are desired in new products for application in the industrial control space.

System Protection Profile for Industrial Control Systems (SPP-ICS) Document

The System Protection Profile for Industrial Control Systems (SPP-ICS) [6] document is an extension of the ISO/IEC 15408 Common Criteria to support integrated systems. This document is designed to present a cohesive, cross-industry, baseline set of security requirements for the procurement of new industrial control systems. The SPP-ICS considers an entire system and addresses requirements for the entire system lifecycle. The SPP-ICS also acts as a starting point for more specific system protection profiles for a specific instance of an industrial control system, such as a DCS or a SCADA system, and for component protection profiles, such as industrial controller authentication or sensor authentication.

The SPP-ICS specifies the integrated set of security requirements for industrial control systems. The integrated set of requirements includes requirements for operating policies and procedures, requirements for information technology based system components, requirements for interfaces and interoperability between system components, and requirements for the physical environment and protection of the system.

Because the SPP-ICS represents an integrated view of the requirements, special consideration is given to decomposition of security functionality and assignment of specific security functions to sub-systems or components of the overall integrated system. The goal of this aspect of analysis and design is to define security requirements for subsystems or system components at the lowest possible level while at the same time retaining the required level of assurance and security functionality for the integrated system as a whole.

In accordance with the CC approach, a boundary called the System Target of Evaluation (STOE) is defined to provide a context for evaluation of the system. The STOE includes both IT and non-IT based security components implemented via policies and operating procedures that are designed to meet the system security objectives and hence counter threats to the ICS. Particular detail is given to the interaction and dependencies between the security subsystem and the overall industrial control system.

The scope of the STOE for the SPP-ICS is depicted graphically in Figure 2. The boxes depict the primary system security functions. These functions are user authentication services (including user access control), physical access control, boundary protection, and data/device authentication. User authentication services control access to industrial control related computer systems including the HMI and remote diagnostics and maintenance. In addition, user authentication is used by the physical access control system to authenticate personnel for physical access. Data/device authentication is shown as a separate function to emphasize the need for data and command signal authentication. Note that the corporate intranet is in the external environment of the STOE. The lines from actuator to controlled process and from controlled process to sensor indicate that these are physical connections representing the direct interactions that take place. The rest of the diagram depicts logical connections. Security controls based on management and operating procedures are not shown in the figure.

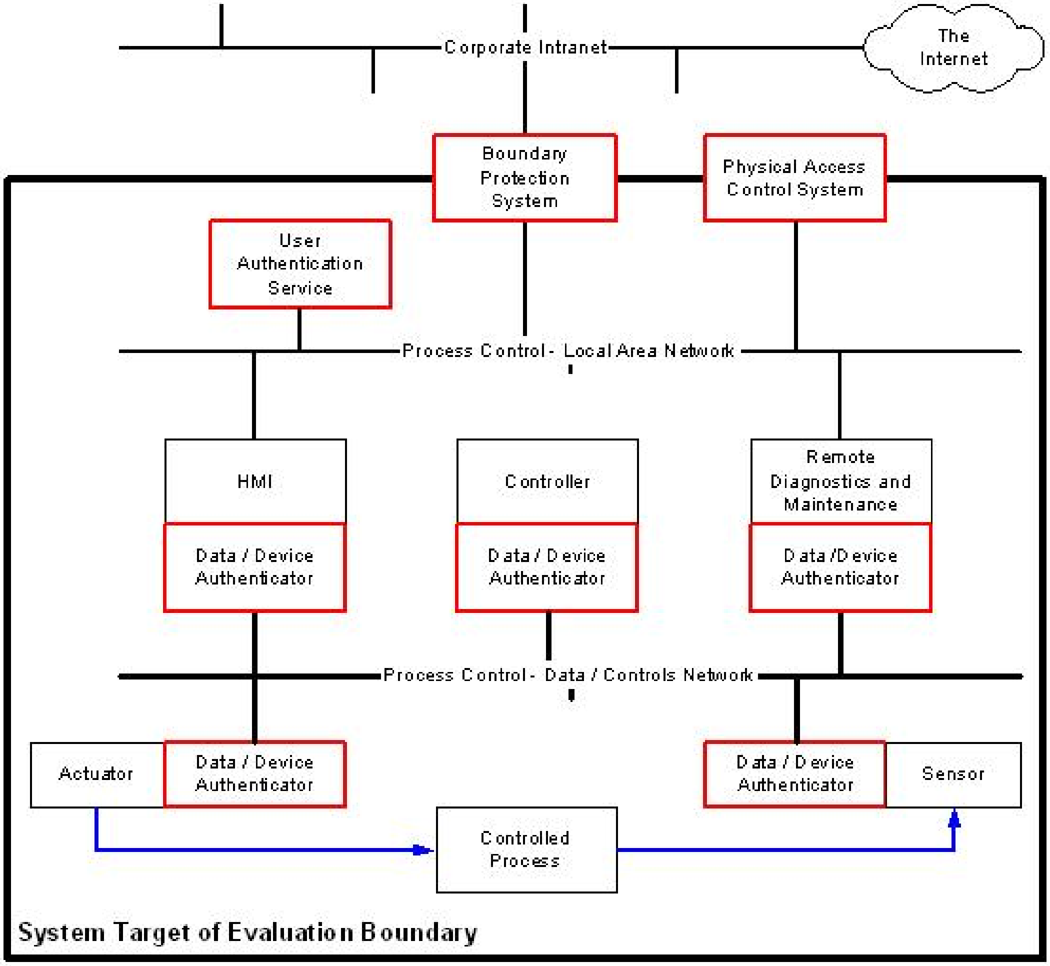
Corporate Intranet
The Internet
Boundary Protection System
Physical Access Control System
User Authentication Service
Process Control - Local Area Network
HMI
Controller
Remote Diagnostics and Maintenance
Data / Device Authenticator
Data / Device Authenticator
Data /Device Authenticator
Process Control - Data / Controls Network
Actuator
Data / Device Authenticator
Data / Device Authenticator
Sensor
Controlled Process
System Target of Evaluation Boundary

Figure 2 - SPP-ICS System Target of Evaluation

ISA SP-99

The Instrumentation, Systems, and Automation Society (ISA) is a global, cross-industry organization that includes representatives from all process control sectors. ISA SP-99 is the Manufacturing and Control Systems Security Committee in the ISA. The committee was formed in the fall of 2002 to establish standards, recommended practices, technical reports, and related information that will define procedures for implementing electronically secure manufacturing and control systems and assessing electronic security performance.

NIST PCSRF requirements definition efforts and performance methods work are closely coupled with ISA SP-99 activities and the two organizations stay in close contact. While the specifications being addressed by PCSRF using the Common Criteria are directed towards the procurement of new industrial control systems, there is substantial overlap in addressing security for legacy systems often addressed by SP-99 efforts. Performance test methods developed using the NIST testbed can be readily disseminated through SP-99 security performance activities.

NIST INDUSTRIAL CONTROL SECURITY TESTBED

Parallel to NIST PCSRF activities, NIST has also developed an Industrial Control Systems Testbed to serve as a platform for validating standards for industrial control security, as well as developing performance and conformance test methods. The testbed is comprised of several implementations of typical industrial control and networking equipment as well as relevant sensors and actuators. Current testbed activities are focused on the development of performance metrics and tests that industry can use to mitigate potential problems encountered during the deployment of security software and hardware in industrial control system environments.

The two primary testbed implementations emulate a water distribution control system and factory control system, are shown in Figure 3. The network is divided into two subnets where one subnet supports the distribution system and is protected by a software based firewall and the other supports the factory system and is protected by a hardware based firewall. These two subnets originate from a border router just after simulated Internet connectivity via a modem/hub device. Since wireless technology is becoming widely used in the industrial controls setting, the network was also equipped with both 802.11 and 802.15 wireless access points.

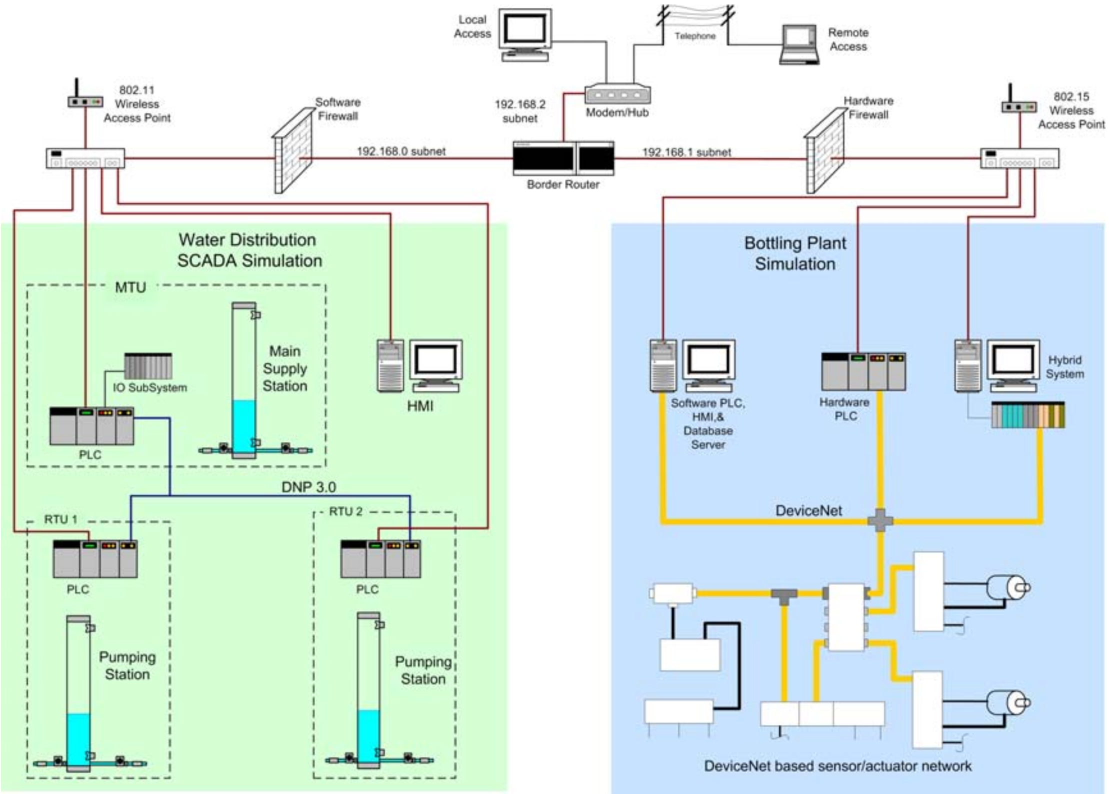

Figure 3 - NIST Industrial Control Systems Security Testbed

The water distribution system, designed to resemble a SCADA system, is shown in Figure 4. The system is comprised of three PLCs. Each PLC controls a tank level via a pump and an ultrasonic level transmitter with the additional capability to monitor tank input and output flows. One PLC serves as the Master Terminal Unit (MTU), a supervisor, and communicates with the two other PLCs that serve as the Remote Terminal Units (RTUs), field subordinates to the supervisor. The MTU supplies water from its tank to meet the demands of the two RTU controlled tanks. Water drained from the RTU tanks simulates user demand on the distribution system. The water distribution simulation is closed so that water drained from the RTU tanks is fed to a holding tank to again be used to fill the MTU main supply tank. The entire SCADA system is controlled by a HMI based supervisor running on a PC. The HMI is interfaced to the MTU via Ethernet. The RTUs communicate to the HMI through the MTU. MTU/RTU communication capabilities include Ethernet or serial using the Distributed Networking Protocol version

3.0 (DNP 3.0). This system was built entirely with commercially available equipment including PLC hardware and software, HMI software, software interfaces, sensors and actuators.

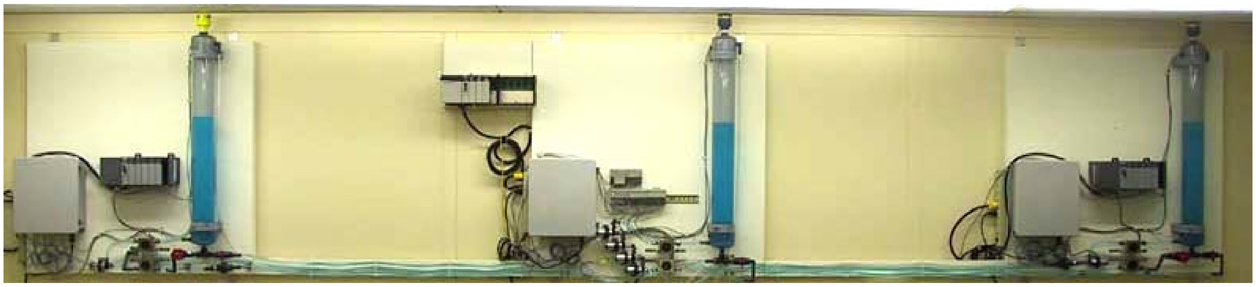

Figure 4 - Water Distribution SCADA System

The factory control simulation, designed to resemble a bottling plant, is shown in Figure 5. It uses industrial conveyor modules arranged to form a loop of continuously circulating bottles. The conveyor system has a station that senses and ejects bottles that are not labeled. Conveyor drives as well as an eject station actuator and sensors are interfaced to the system controller using a DeviceNet network. DeviceNet is an open communication standard used to connect devices such as sensors and actuators to PCs and PLCs. DeviceNet, one of several intelligent control networking technologies available, allows industrial devices to be easily networked and managed remotely. The conveyor hardware and sensor network has been integrated so it can optionally be controlled by one of three controllers. The controllers include a typical hardware PLC, a software based PLC that runs on a PC, and a Hybrid Control System (HCS) all interfaced through DeviceNet. A Hybrid Control System is supplied as a fully integrated a system operating as a PLC, an HMI and a data historian. In addition to the data historian contained with the HCS, the testbed also contains an additional data historian software application.

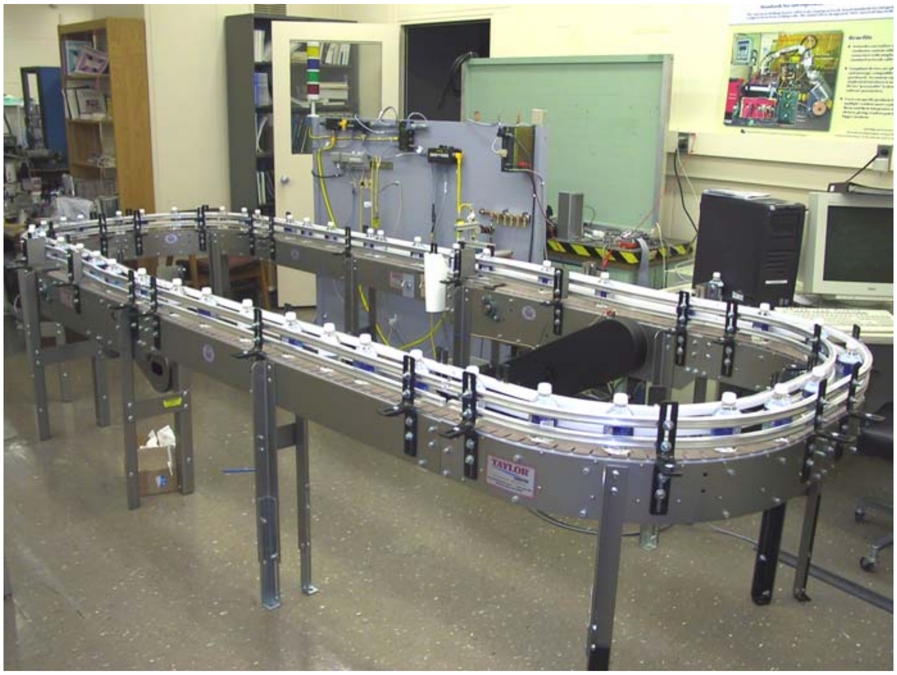

Figure 5 - Bottling Plant Simulation

PERFORMANCE TESTING OF SECURITY IMPLEMENTATIONS

Security Software and Concurrently Executing Control Software

NIST is using the industrial control security testbed to evaluate the impact of security solutions on the sensitive timing requirements of industrial control systems. Efforts are currently focused on developing test methods to characterize the performance control software execution relative to modes of operation of concurrently executing security software. Industry interests have focused initial methodology development to evaluate the effects of anti-virus (AV) software packages running concurrently with HMI software. NIST has conducted initial performance tests using an HMI software package and a commercially available AV software application. The test methodology used as well as the data collected were presented to industrial collaborators and feedback was collected. This test methodology is currently being refined and more detailed testing will be conducted. Once the test methodology nears completion, it will be used to test additional HMI and anti-virus applications. Data will be made application generic and presented to the industry with the methodology. It is also expected that this work will be extended to include other security software applications, such as personal firewalls, and more time-critical control applications, such as software based PLCs.

The test setup for development of this methodology uses the water distribution SCADA testbed. Initial data presented here was collected using an HMI application running concurrently with an AV application on a PC with a 450MHz Pentium processor. The PC also contains the IO Server, an application that serves as a communication proxy between the HMI and the PLC. The SCADA system is configured using Ethernet communications as described in the testbed section above. The HMI is currently configured with 12 monitoring and control variables (tag points). Ethernet packet data was recorded over time intervals that were dependent on the length of time required to carry out the anti-virus operation. The data was then analyzed with some custom software to extract the time between subsequent packets for a single sensor variable being communicated between the MTU PLC and the HMI.

Preliminary Test Results

A baseline messaging time of 150 ms was established between the HMI and the MTU PLC with no anti-virus software executing. Tests were then performed over the following anti-virus modes of operation:

- Manual Scanning – the application’s virus scanning process scans a group of directories and files for viruses as a user initiated manual operation or automatically based on some time interval.
- Real-Time Scanning – the application’s virus scanning process continually monitors the system for file activity. File activity typically includes data access, copy, save, move, open and close operations. Once activity is detected the files or data associated with the activity are scanned.
- Virus Definition Update – an operation that updates an application’s listing of virus signatures.

During real-time and manual scanning tests, the EICAR test virus [7] was injected into various access points on the HMI PC.

Figure 6 shows the results of performing manual scans on 2.3 Gbytes of hard disk space that contains three instances of the EICAR virus: a text file, an archived file and a double archived file. Note that most anti-virus software packages can be configured to look for viruses within archived files several layers deep. During initialization of the scanning process, the time between consecutive packets increases from 150 ms to almost 400 ms, however, once initiated, there is no significant impact on the communication performance in the current test configuration. The particular anti-virus software used during this testing allows a user to set its process priority, a setting that is set to minimum as a default. As this setting was increased, there were significant delays in control packets between the HMI and MTU PLC. When set to the highest priority, the HMI/PLC communications essentially came to a halt until all manual scanning was completed.

Figure 7 displays results of dragging and dropping a virus infected directory from the floppy drive to the hard drive while in real-time scanning mode. Like in the above hard drive scan, the viruses are detected and quarantined with no significant effect on communication performance. Figure 8 indicates an increase from 150 ms to approximately 400 ms over the duration of a 1.5 minute virus definition update.

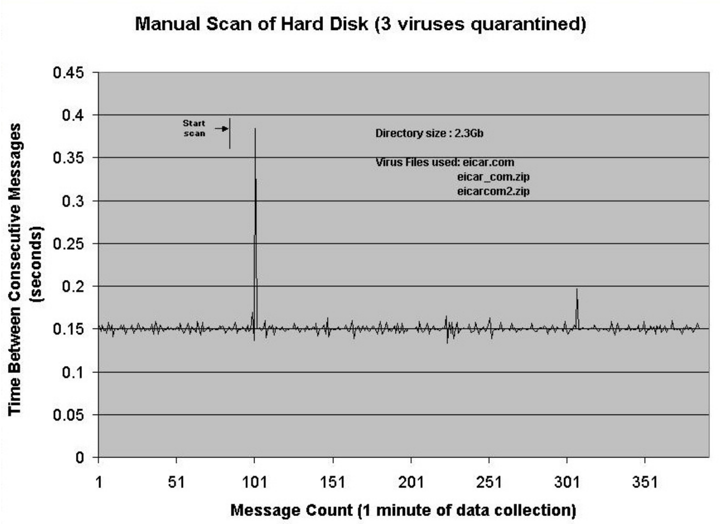

Figure 6 – Manual Scan Data

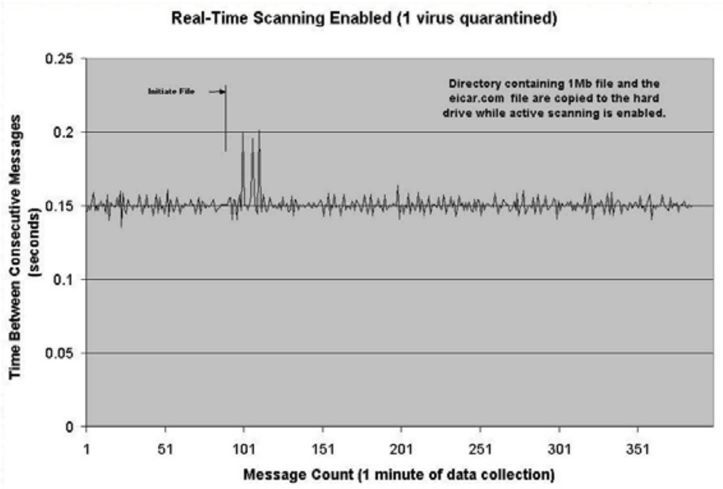

Figure 7 – Real-Time Scan Data

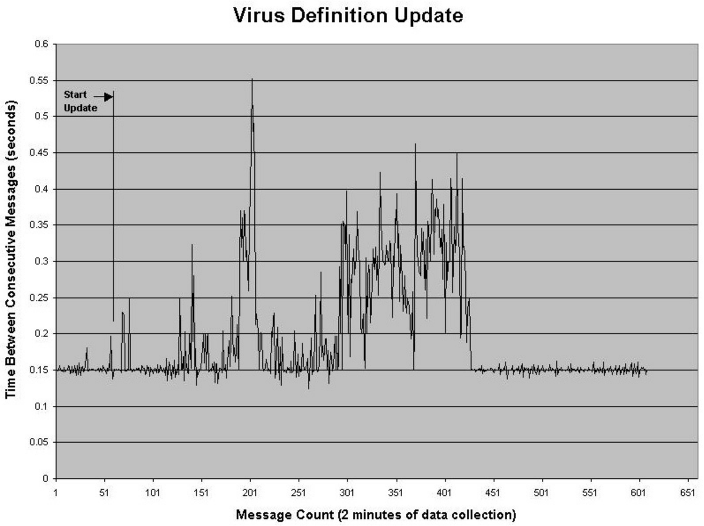

Figure 8 - Virus Definition Update Data

Current Status

The test methodology used as well as the data collected were presented to industrial collaborators. Feedback is being collected and used towards continued developments of the methodology. The following are some key observations and feedback based on initial test results.

- Actual detection and associated operation of quarantining a virus appears to have no significant effect on HMI performance.
- Increasing the anti-virus process priority setting indicated that processor load has a significant effect on HMI performance.
- In addition to monitoring packet communication delays, the test methodology should also specify to monitor PC system resources such as CPU usage.
- The test methodology should be expanded to include tests simulating a heavily loaded HMI application (i.e. large number of data points and scripts).
- The test methodology should be expanded to include the effect of data historian traffic during real-time scanning.
- Industry reports that legacy systems are still using processors in the 300 MHz range, additional testing should be performed on lower and higher end machines in addition to the current 450 MHz PC that is being used.
- Once a more inclusive test methodology is defined, additional HMI and anti-virus applications must be tested.

When fully developed, the methodology will contain a series of tests and suggestions for integrators to use when applying anti-virus protection applications on systems running HMI software. While the methodology will not be specific to any one anti-virus or HMI application, it will present test procedures to determine if the integrated security solution affects a system's performance. In addition, the methodology will provide example data and also offer suggestions for possible system configurations or suggest that functions be performed during minimal system activity. In addition, industry collaborators expressed interest in developing similar test methods for other host based security applications such as personal firewalls and for software based PLCs. Software PLCs provide the same functionality as hardware based PLCs, however, they are implemented in software on a PC. It is expected that concurrently executing security software will have the greatest impact on the performance of these systems since real-time cycles are often within (10 to 50) ms.

Cryptographic Modules and SCADA Communication Networks

Cryptographic modules are being produced in accordance with cyber security standards and protocols being developed by the American Gas Association, AGA-12 committee [8]. These modules are designed for placement in series between the RTU and MTU components of a SCADA system. The utility industries must understand how integration of these security components into SCADA systems affect data communication performance. To assist industry, NIST has contracted the Gas Technology Institute (GTI) to develop detailed test methods for evaluating the impact of cryptography on SCADA system communication performance. GTI is contracted to specify a test protocol, validate it in a laboratory setting, carry out field measurements, and analyze and publish the data. Upon completion of the contract, GTI will provide NIST with the developed test methodology, laboratory and field test results and a set of SCADA link encryption modules. NIST will perform validation tests on the test methodology using the cryptographic modules on its testbed. Figure 9 shows the laboratory testbed GTI has constructed for conducting cryptographic module performance testing.

PERFORMANCE METRICS AND TESTS FOR INDUSTRIAL ETHERNET I/O

Industrial networks such as DeviceNet, Modbus and Profibus are specifically designed to meet the performance characteristics required in industrial networks. Because of these requirements, these networks are limited in speed and length and are designed around a fixed network architecture. Ethernet, until recently, was not considered a viable choice for industrial networking due primarily to its determinism limitations. However, Ethernet has progressed considerably since its original design. Its inherent collision problems have been eliminated through transition from half-duplex to full-duplex networking and new network architectures have been recommended for industrial implementations. New protocols, such as EtherNet/IP (Ethernet / Industrial Protocol), are also enabling industry to accept Ethernet as a viable industrial network. NIST is helping industry to gain confidence in Ethernet as an alternative industrial network solution by working with the Open DeviceNet Vendor Association (ODVA) to develop a set of metrics and tests for real-time I/O performance of EtherNet/IP based industrial devices [9]. These metrics and tests will help users to compare the performance metrics between devices without having to understand the internal details of each device. While these tests are currently being developed for EtherNet/IP, they are generic enough as to be applicable to all industrial Ethernet. From a security perspective, these metrics and tests will be used to establish baseline performance for a particular device and then determine the performance degradations induced by the integration of security technologies.

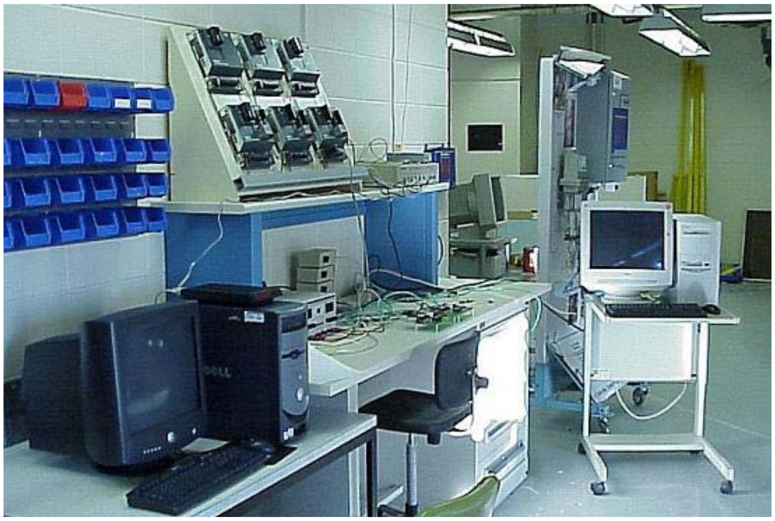

Figure 9 - GTI Laboratory Testbed

Leveraging Performance Standards

These industrial Ethernet performance efforts are leveraging existing standards for networking technology. RFC 1242 (Benchmarking Terminology for Network Interconnection Devices) and RFC 2544 (Benchmarking Methodology for Network Interconnect Devices) are two Internet Engineering Task force (IETF) Request For Comment (RFC) documents being used for these efforts. Most, if not all, networking infrastructure devices (e.g., switches, routers, hubs, and bridges) are tested against these two RFCs.

NIST and ODVA have borrowed four definitions in particular from RFC 1242 that provide a common set of terminology to describe both the tests and results. These terms are:

- **Throughput –** The maximum continuous traffic rate a device can send/receive without dropping a single packet (frames per second at a given frame size).
- **Latency –** The time interval between a message being sent to a device and a corresponding event occurring.
- **Jitter/Variability –** The amount of change in the measured times for a series of events. This measure includes the difference between the minimum and maximum values as well as the standard deviation of the measured times.
- **Overload Behavior –** A qualitative description of the behavior of a device in an overload state.
    - Overload states exist when the device’s internal resources either receive too much information to process or bad information and the device goes into a state other than its normal run mode.
    - Data recorded for overload states should:
        - Describe the device behavior when its resources are exhausted.
        - Describe the system management response in an overload state.
        - Describe the device recovery from an overload state.

NIST and ODVA have also added two modifications to the Latency term.

- **Response Latency –** The closed-loop latency of a device to process a command and respond to it (e.g. a request for the device's serial number).
- **Action Latency –** The closed-loop latency of a device to process a command and return a desired physical output (e.g. analog/digital output signal), or the closed loop latency of a device to process a physical action (e.g. analog/digital input signal) and return a response.

Testbed Setup

Leveraging equipment from the water distribution system described above, NIST has implemented a basic set of equipment that is being used to develop performance tests for EtherNet/IP networks. This equipment includes an industrial PLC with multiple network interfaces and a distributed I/O system with digital and analog I/O modules. Also used in this test setup is a high speed network analyzer and traffic generator capable of making timing measurements with accuracies of 100 ns and producing 1000 independent network streams at beyond wire-rate. A diagram of the performance testbed is shown in Figure 10.

Performance testing methodologies

NIST has developed some basic methodologies to test the performance of EtherNet/IP. The producer/consumer model for EtherNet/IP allows multiple modes of communication to be chosen for real-time data exchange. The most common mode for producing data is called cyclic production. During cyclic production, the producer will send data at a particular rate called the Requested Packet Interval (RPI). The RPI, and corresponding Accepted Packet Interval, dictates the speed of the data produced over the network regardless of the rate at which the actual data values change. A device's ability to maintain that RPI value is an important variable in control system operation. Since the RPI is the basis for most of the real-time I/O communications over EtherNet/IP, a test method was developed to measure it using packet analysis.

As mentioned earlier, NIST and ODVA have developed two modifications to the latency term for testing industrial devices. These tests relate to actual inputs and outputs to and from a device, and are the most relevant real-world tests for determining the performance characteristics of an industrial control communications network. NIST is working on the development of test methodologies that can gage these metrics.

EtherNet/IP Interoperability Plug-Fests

In addition to the development of metrics and tests for industrial Ethernet, NIST has collected and analyzed data from two ODVA sponsored EtherNet/IP Interoperability Plug-Fests. These plug-fests provide a collaborative environment where any vendor developing an EtherNet/IP product can participate to determine how interoperable their device is with other vendor products. This activity determines how well participants conform to the EtherNet/IP specification and helps to identify ambiguities within the specification.

During interoperability testing activities, data was collected on the performance of the different devices. Since the performance tests were not the main focus of the event, only the cyclic/RPI producer testing was performed. This allowed the performance test equipment to remain a passive component in the system, while not disturbing the interoperability testing. Test results indicated that none of the devices performed exactly the same. NIST identified different characteristics in the data and determined possible causes for their occurrence. One characteristic indicates whether a device uses a hardware or software clock. The spike pattern in the data sets are usually related to some overhead in the processor that caused a packet to be delivered late showing up as an upward spike on the graph. For devices using a hardware clock for their RPI timing, the next packet showed a subsequent early packet after each late packet, resulting in a downward spike at almost the same distance. The device returning to the original RPI sequence time caused the downward spike. Devices that use a software clock for their RPI timing did not show this downward spike. Their timing was always calculated based on the time the last packet was sent. Figure 11 shows example data from two devices, one with a hardware clock and one with a software clock.

Tests performed also made it possible to determine the clock resolution used by some devices. These devices tended to be software clock devices, since hardware clocks run at significantly higher frequencies than could be measured using the current test equipment. The data for software clock resolution showed large blocks of spikes with easily identifiable steps in the data. Figure 12 shows an example of a device that uses a software clock and has a clock resolution easily identifiable from the spike pattern.

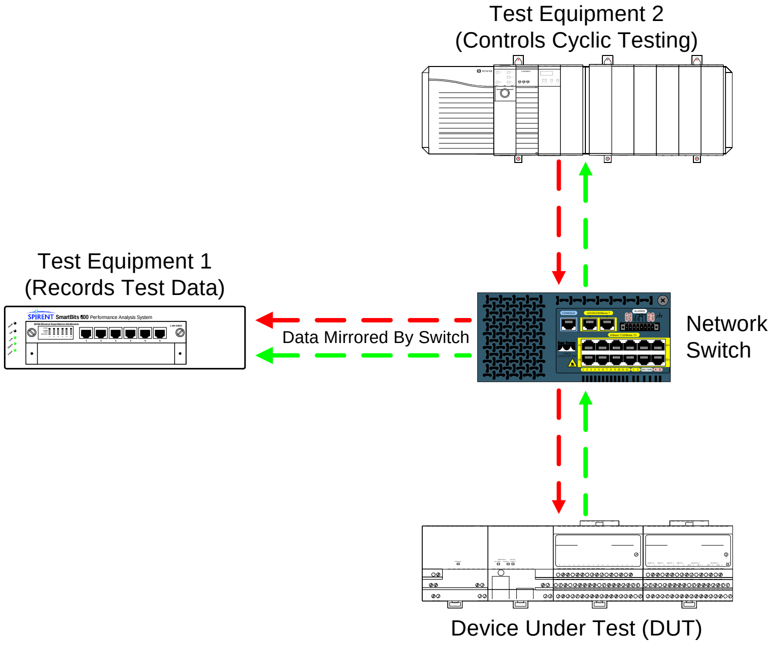

Figure 10 - EtherNet/IP Performance Testbed Layout

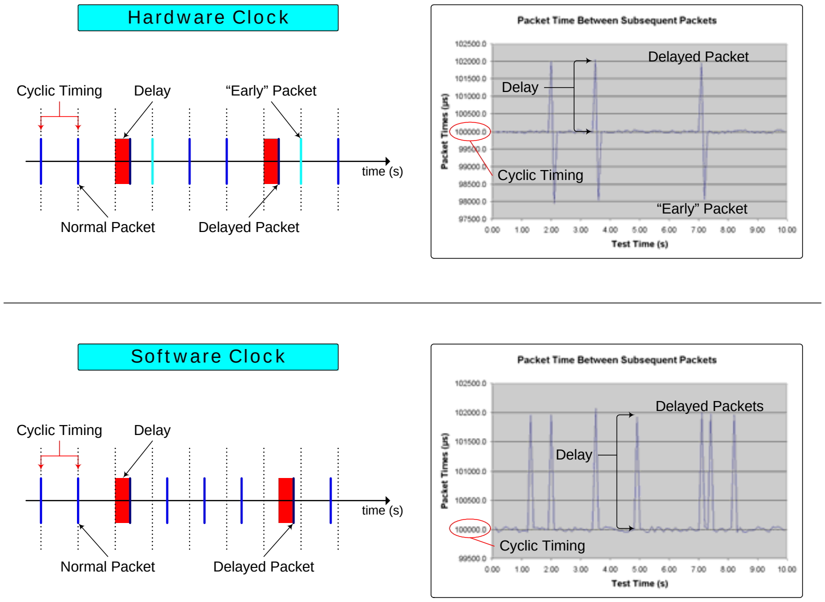

Figure 11 - Example Data Showing Devices With Hardware & Software Clocks

This work with ODVA to leverage IT-based metrics and tests for Ethernet device performance to describe the performance of industrial Ethernet devices is beneficial, since a great amount of work has gone into developing these standards. However, it is anticipated that the metrics and tests for industrial Ethernet devices are going to be substantially different due to the limitations of industrial devices. Also, the methodologies developed for industrial

Ethernet performance will require different implementations from device to device. Yet, given the benefits to users, who at this point have very limited ways to compare similar products from multiple vendors, it is necessary to try and standardize as much of these metrics and tests as possible.

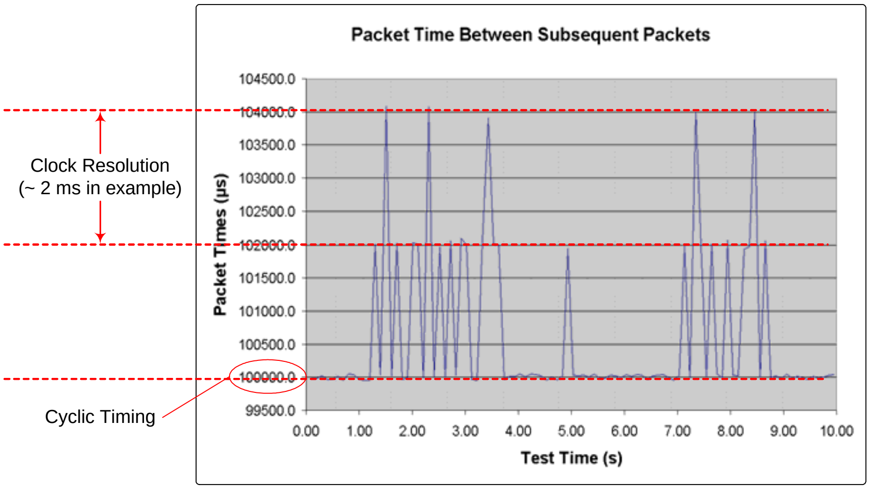

Figure 12 - Example Data Showing Software Clock Resolution

SUMMARY

The National Institute of Standards and Technology is defining and applying standard information security requirements and developing laboratory and field test methods for information security products and approaches to secure industrial control systems while maintaining their critical operational requirements. To help US industry define security requirements, NIST has initiated an industry wide group called the Process Controls Security Requirements Forum. The PCSRF is developing its security specifications using the Common Criteria and to date has produced two documents, the Security Capabilities Profile and the System Protection Profile for Industrial Control Systems, as an industry-centric starting point towards more industry specific system requirements. Parallel to PCSRF efforts, NIST has developed a laboratory scale testbed comprised of several implementations of typical industrial control and networking equipment as well as relevant sensors and actuators. This testbed is being used to develop performance test methods that can be applied to process control security products to determine if particular time-sensitive requirements can be met. Initial developments in the areas of security software and hardware implementation test methodologies as well as performance metrics and tests for industrial Ethernet I/O were presented.

REFERENCES

1. Critical Infrastructure Protection, Challenges in Securing Control Systems, United States General Accounting Office (GAO), Statement of Robert F. Dacey, Director, Information Security Issues, Testimony Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, House Committee on Government Reform, .October 1, 2003, http://www.gao.gov/

2. Falco, Stouffer, Wavering, Proctor, IT Security for Industrial Control Systems, NISTIR 6859, February 2002.

3. Process Control Security Requirements Forum (PCSRF), http://www.isd.mel.nist.gov/projects/processcontrol/

4. Common Criteria for Information Technology Security Evaluation, "Part1: Introduction and general model, CCIMB-99-031, Version 2.1," 1999.

5. Security Capabilities Profile (SCP), September 17, 2003 http://www.isd.mel.nist.gov/projects/processcontrol/members/documents/SCP-17-Sep-03.doc

6. System Protection Profile for Industrial Control Systems (SPP-ICS) Version 0.91, February 4, 2004 http://www.isd.mel.nist.gov/projects/processcontrol/members/documents/SPP-ICS-v0.91.doc

7. The EICAR Anti-Virus Test File, http://www.eicar.org/anti_virus_test_file.htm

8. AGA draft standard, Cryptographic Protection of Existing SCADA Systems, http://www.gastechnology.org/webroot/downloads/en/1ResearchCap/1_1GasOps/AGASCADANews.pdf

9. J. Gilsinn, Real-Time I/O Performance Metrics and Tests for Industrial Ethernet, ISA Automation West, 2004. http://www.isa.org/