The NIST Process Control Security Requirements Forum (PCSRF) and the Future of Industrial Control System Security

Keith Stouffer, Joe Falco, Fred Proctor
National Institute of Standards and Technology (NIST)

To be presented at 2004 TAPPI Paper Summit
Atlanta, Georgia, May 3-5, 2004

ABSTRACT

This paper will provide an overview of the Process Control Security Requirements Forum (PCSRF) and the System Protection Profile for Industrial Control Systems (SPP-ICS) document. The SPP-ICS presents a cohesive, cross-industry, baseline set of security requirements for new industrial process control systems. It is based on the ISO/IEC 15408 Common Criteria, a widely used standard for defining traditional IT security requirements. The SPP-ICS can be combined with specific pulp/paper security requirements to produce a document that addresses future security requirements for the pulp/paper industry.

INTRODUCTION

The widespread use of IT for remote monitoring and control of the electric power system and for controlling industrial processes in the oil and gas, water, chemical, pharmaceutical, food and beverage, pulp and paper, and other industries, has unintentionally introduced security vulnerabilities. The National Institute of Standards and Technology (NIST) is working with process control end users, vendors and integrators to improve the IT security of networked digital control systems used in industrial applications. This effort is being carried out through the Process Control Security Requirements Forum (PCSRF).

The PCSRF is a working group of representatives from the various sectors that make up the process control industry and the vendors that design, produce, and/or integrate components and systems for the industry. 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. process controls industry would employ through a combination of IT and non-IT mechanisms to reduce residual risk 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 Common Criteria Protection Profile security specifications. The primary focus area of the group to improve the IT security of the computer control systems used in process industries, including electric utilities, petroleum (oil and gas), water, waste, chemicals, pharmaceuticals, pulp and paper, and metals and mining with an emphasis on industries considered to be part of the nation’s critical infrastructure.

Securing these systems is a challenge. These systems are often time critical and are designed to maximize performance, reliability, flexibility, and safety. It can be difficult to balance these characteristics with security. Safety is the number one concern and security requirements cannot compromise the safety requirements of the system.

In the past, these systems have typically been physically isolated and based on proprietary hardware and communications. Therefore, security has not been a significant consideration. Today, these systems are often connected to the corporate and business networks, use open/Commercial-Off-The-Shelf (COTS) components and are connected via Ethernet. This increased connectivity and use of common components is often very beneficial, but also increases the vulnerabilities of these 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.

ISA-SP99 – ADDRESSING THE INSTALLED BASE

The Instrumentation, Systems, and Automation Society (ISA) is a global, cross-industry organization that includes representatives from all process control sectors. The focus of the organizations is more on Distributed Control Systems (DCS) and plant floor operations than Supervisory Control and Data Acquisition (SCADA) systems, but all process control disciplines are represented in this large organization.

ISA-SP99 [1] 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 security practices and assessing electronic security performance. Guidance is directed towards those responsible for designing, implementing, or managing manufacturing and control systems and also applies to users, system integrators, security practitioners, and control systems manufacturers and vendors.

Initially, ISA-SP99 has focused on documenting guidelines and considerations for control system security in two Technical Reports (TR): WG1/TR1 "Technologies", and WG2/TR2 "Application and Practices." The draft Technical Reports incorporate a great deal of information from other security standards and publications and add information specific to control systems. These Technical Reports are useful for identifying issues to consider and should be available for purchase in the near future.

PCSRF – ADDRESSING THE FUTURE

To address the future security requirements for industrial process control systems and components, NIST formed the Process Control Security Requirements Forum (PCSRF) [2] in the spring of 2001. The PCSRF is a working group of users, vendors, and integrators in the process control industry who are concerned about information security in an increasingly networked world. The PCSRF addresses the cyber security requirements for industrial process 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.

Members of the PCSRF represent the critical infrastructures and related process industries, including oil and gas, water, electric power, chemicals, pharmaceuticals, metals and mining, and pulp and paper. There are currently over 400 members in the PCSRF from government, academic and private sectors, including ABB, Emerson Process Management, Honeywell, Invensys, Rockwell, Cisco, Microsoft, Sun Microsystems, American Gas Association, BP, Chevron Texaco, Exxon Mobile, Association of Metropolitan Water Agencies, American Chemistry Council, Dow, Dupont, Eastman Kodak, Schering-Plough, Georgia-Pacific, I-4, ISA, National Defense University, Idaho National Engineering & Environmental Lab, Pacific Northwest National Lab, Sandia National Lab, Department of Homeland Security, National Security Agency and NIST.

The main goal of the PCSRF is to increase the security of industrial process 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.

Security Capabilities Profile (SCP) Document

The first document developed by PCSRF was the Security Capabilities Profile (SCP) [3]. The SCP is a document that serves as a means to reach consensus within and across the various industries regarding the security capabilities that are required in a secure industrial process control system. The document also serves as a vehicle to convey to the process control system and component vendors the security capabilities that are desired in new products for application in the industrial process control space.

During initial information gathering exercises, the PCSRF identified vulnerabilities across the boundaries of the diverse participating industries. Industry specific working groups defined vulnerabilities specific to their process control system based on a minimal set of system functions and capabilities defined by the PCSRF. The results of the individual vulnerability assessments were analyzed and consolidated, by the PCSRF, 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 risks 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 in the same manner as requirements and assurance measures are selected to meet a Safety Integrity Level (SIL) as in IEC 61508 [4].

The SCP and its derivatives will also serve as a basis for developing ISO/IEC 15408 Common Criteria compliant Protection Profiles to aid in development and verification of the security capabilities of industrial process control systems and components.

Common Criteria Based Approach

The Common Criteria (CC), ISO/IEC 15408 [5], is a meta-standard of criteria and constructs used to develop security specifications in support of the evaluation of products. 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.

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 systems. This document is designed to present a cohesive, cross-industry, baseline set of security requirements for the procurement of new process 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 (SCADA, DCS), for a specific instance of an industrial control system, and for component protection profiles (industrial controller authentication, sensor authentication, etc).

The System Protection Profile for Industrial Control Systems (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.

As shown in Figure 1, a generic industrial control system [7] consists of classes of components for the direct control of a process (the controller(s), actuators and sensors), a Human Machine Interface (HMI), and capabilities for remote diagnostics and maintenance. 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 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. Although not represented in the diagram, there are also human elements such as operators and non-technical elements such as operating procedures.

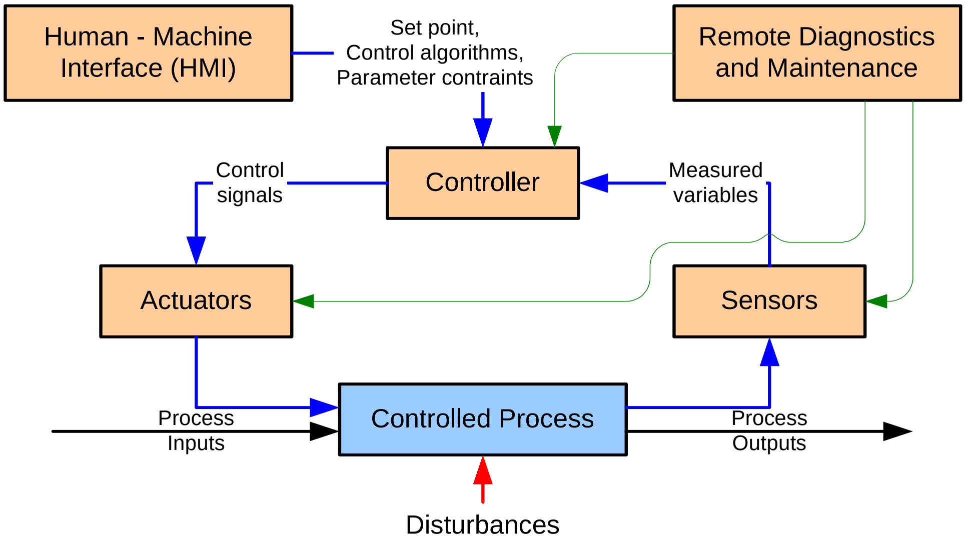

Figure 1 Generic industrial control system

To provide a context for evaluation of the system, a boundary called the System Target of Evaluation (STOE) must be defined. The STOE includes both the information technology based components and the non-information technology based elements implemented via policies and operating procedures, which are designed to meet the security objectives defined to counter threats to the ICS. Particular attention is given to the interaction and dependencies between the security subsystem and the overall industrial control system.

The STOE focuses on protecting data integrity and system availability without interfering with safety system functions. Data integrity centers on protecting data flows to and from the controller and the other ICS components or subsystems. The STOE is also intended to protect system availability to assure continuity of operations. Confidentiality beyond that required to protect the security subsystem itself or to protect against specific attacks on the ICS is not considered to be a large risk.

The scope of the STOE 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 process control related computer systems including the human machine interface (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.

The SPP-ICS is written for a generic industrial control system as a high-level statement of requirements. It provides a starting point for more specific and detailed statements of requirements for industrial control systems focused on a specific industry, company, or component. Pulp/paper specific security requirements can be combined with the SPP-ICS to produce a document that addresses future security requirements for the pulp/paper industry.

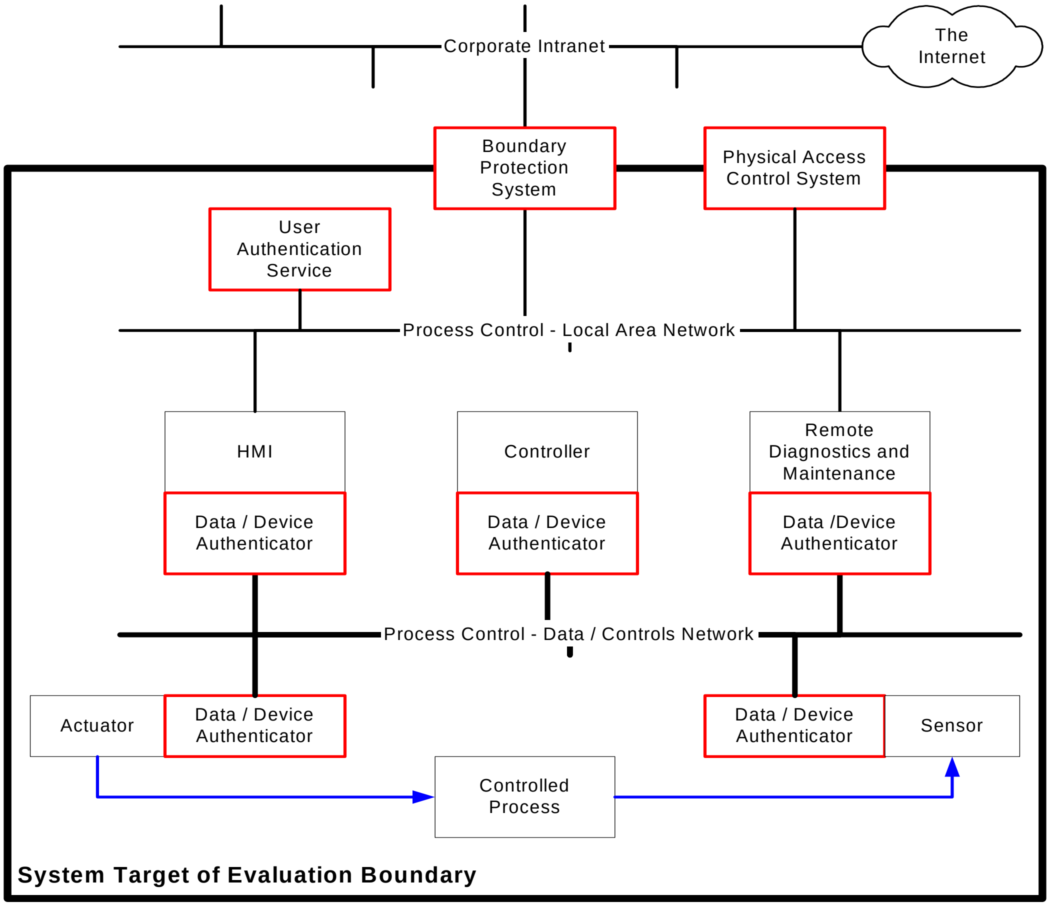
Corporate Intranet
The Internet
Boundary Protection System
Physical Access Control System
User Authentication Service
Process Control - Local Area Network
HMI
Controller
Remote Diagnostics and Maintenance
Data / Device Authenticator
Data / Device Authenticator
Data /Device Authenticator
Process Control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

NIST INDUSTRIAL CONTROL SYSTEMS SECURITY TESTBED

Parallel to NIST PCSRF efforts, NIST has also initiated the development of a testbed consisting of several implementations of typical industrial control systems, networking equipment, as well as relevant sensors and actuators. This Industrial Control System Security Testbed is being used at NIST to develop test methods for validation and conformance testing of security implementations. The testbed is also being used to help identify system vulnerabilities as well as establish best practice guidelines.

The two primary testbed implementations are a water distribution and a bottling plant simulation.
The current network configuration of the NIST Industrial Control Systems Security Testbed is shown in Figure 3. The network is divided into two subnets, where one subnet supports the water distribution simulation and is protected by a software-based firewall, and the other supports the bottling plant simulation 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.

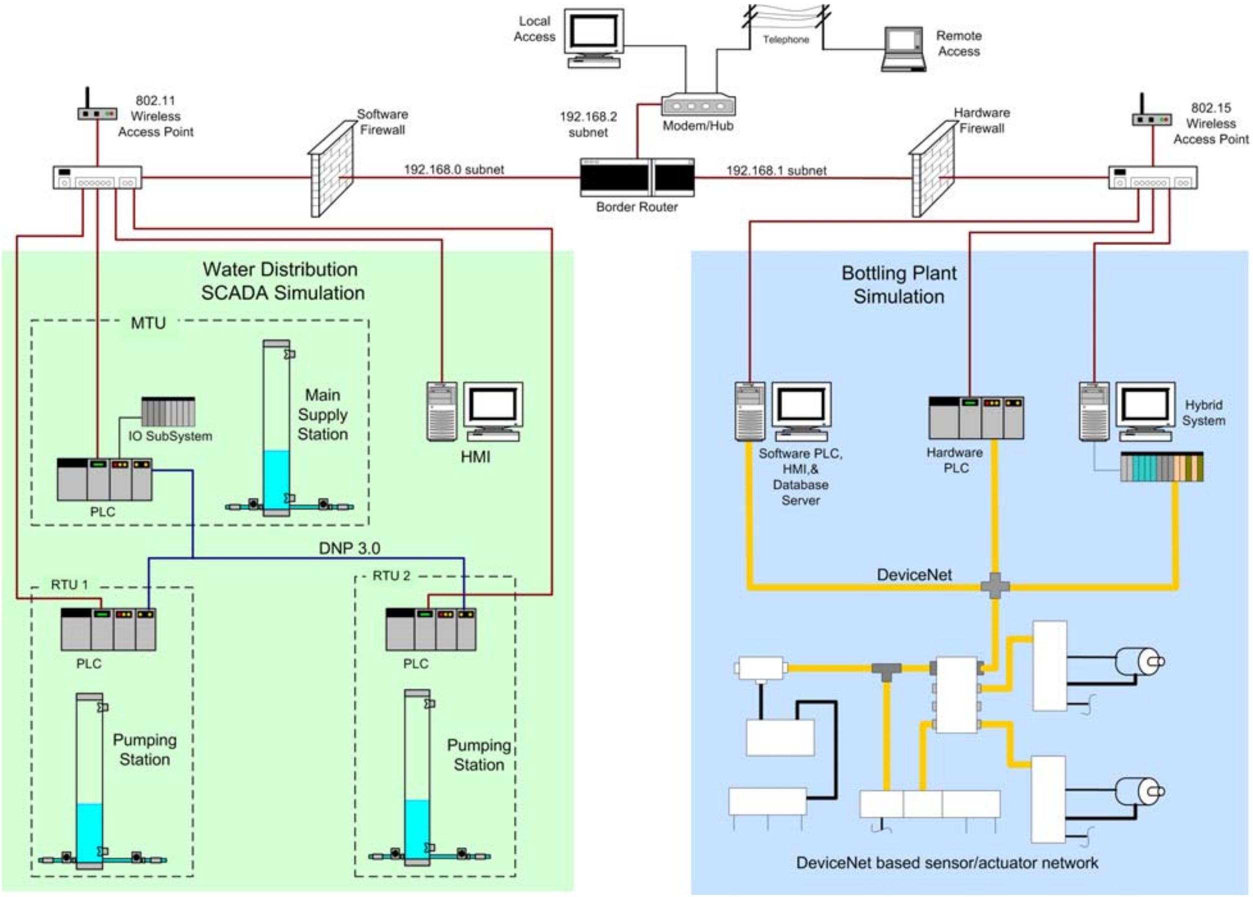

Figure 3 NIST Industrial Control Systems Security Testbed

The water distribution simulation is designed as a SCADA system, and is shown in Figure 4. The system consists 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) and communicates with two other PLCs serving as Remote Terminal Units (RTUs). The MTU supplies water from its controlled 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 controllable via a Human Machine Interface (HMI) running on a PC. The HMI is interfaced to the MTU via Ethernet. Each RTU is interfaced to the HMI through the MTU. MTU/RTU communication capabilities include Ethernet or serial using the Distributed Networking Protocol (DNP) v3.0. The SCADA system was built entirely with commercially available equipment and hardware including PLC hardware and software, HMI software, and software interfaces.

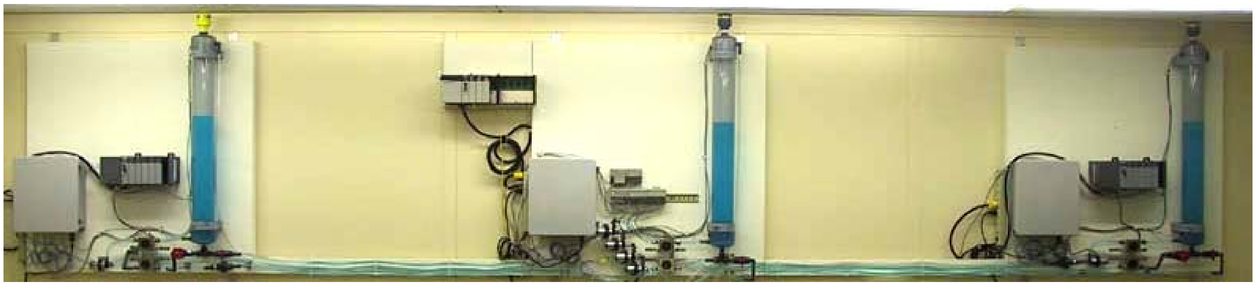

Figure 4 Water distribution SCADA system

The bottling plant simulation shown in Figure 5 uses industrial conveyor modules arranged to form a loop of continuously circulating bottles. The conveyor system has a station that ejects bottle that are missing labels. The conveyor drives, eject station actuator and sensors are interfaced to a DeviceNet network. DeviceNet, one of many industrial network standards, allows industrial devices such as sensors and actuators to be remotely managed by PCs or PLCs.

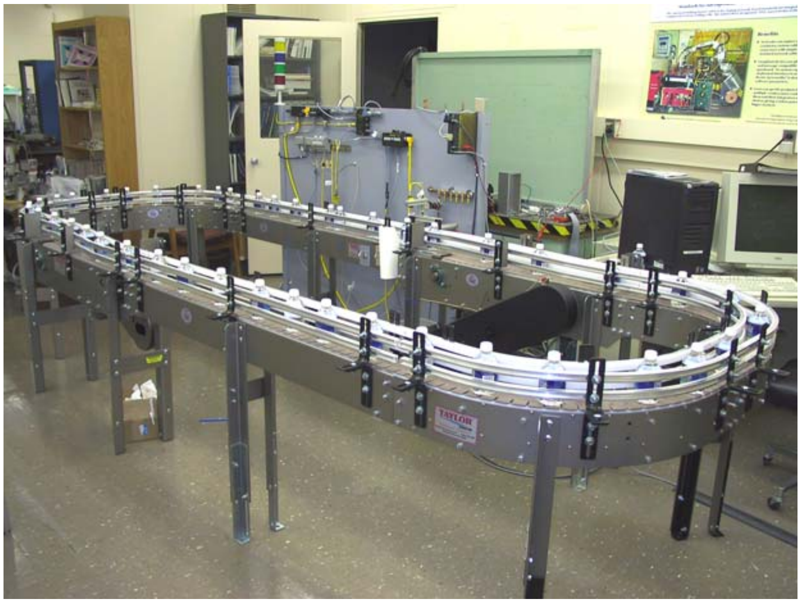

Figure 5 Bottling plant simulation

The conveyor hardware and sensor network has been integrated so it can optionally be controlled by one of three controllers. The controllers include a commercial hardware PLC, a software based PLC that runs on a PC, and a Hybrid Control System (HCS) all interfaced through DeviceNet.

CONCLUSIONS

The main goal of the PCSRF is to increase the security of industrial process control systems through the definition and application of a common set of information security requirements for industrial process control systems using the ISO/IEC 15408 Common Criteria. This will reduce the likelihood of successful cyber-attack on the nation’s critical infrastructures. A system protection profile had been written for a generic industrial control system as a high-level statement of security requirements. It provides a starting point for more specific and detailed statements of requirements for industrial control systems focused on a specific industry, company, or component. Specific pulp/paper specific security requirements can be combined with the system protection profile to produce a document that addresses future security requirements for the pulp/paper industry. A testbed consisting of several implementations of typical industrial control systems is being used at NIST to develop test methods for validation and conformance testing of security implementations.

ACKNOWLEDGMENTS

The authors would like to thank the PCSRF members who provided their time and input to this effort and to Decisive Analytics for their development efforts to produce the SCP and SPP-ICS documents. This effort was funded by the United States Federal Government.

REFERENCES

1. ISA-SP99 **http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821**

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

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

4. IEC 61508 **http://www.iec.ch/zone/fsafety/fsafety_entry.htm**

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

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. Falco, J., Stouffer, K., Wavering, A., Proctor, F., “IT Security for Industrial Control Systems,” NISTIR 6859, February 2002.