Intelligent Systems Programs

Intelligent Manufacturing Industrial Control Systems and Network Standards Program

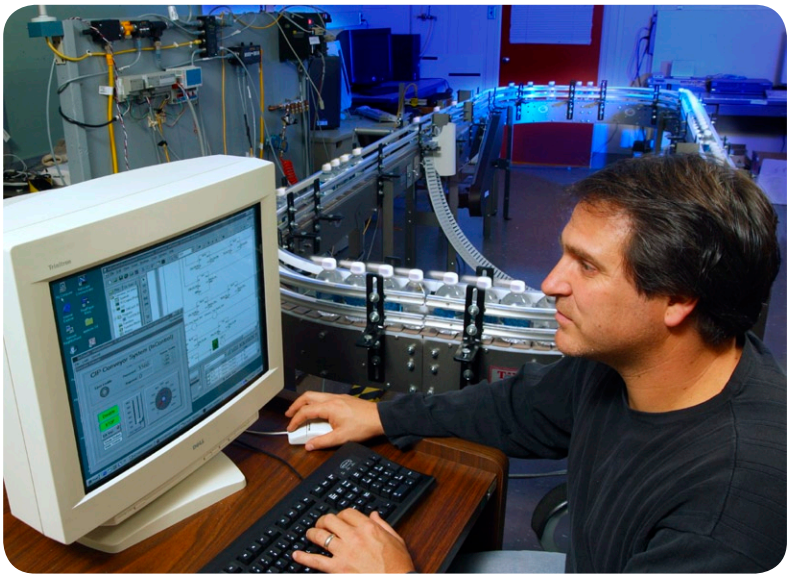
Annual FTEs: 3.5 NIST staff

Challenge

Safe, secure, and reliable industrial control systems are essential for U.S manufacturers and other critical infrastructure. As inter-connectivity grows, the challenges in guaranteeing the security of the most critical systems increase correspondingly.

Overview

Industrial control systems (ICS), including supervisory control and data acquisition (SCADA) systems and distributed control systems (DCS), are an integral part of the U.S. critical infrastructure. The widespread use of general information technologies for remote monitoring and control of electric power generation and distribution systems and pipeline distribution systems; control of industrial processes in the oil and gas, water, chemical, pharmaceutical, food and beverage, pulp and paper, and other industries; and rail and air traffic control, has unintentionally introduced security vulnerabilities. ICS often have to respond in real time and are designed to maximize performance, reliability, flexibility, and safe operation. Typically, these systems link to corporate and business networks, use Open/COTS (Commercial off-the-shelf) components, and are connected via Ethernet. Increased connectivity and use of common components offer a number of advantages, such as reduced costs, but also increase the vulnerabilities and reduce the predictability of these systems. This program capitalizes on extensive achievements from NIST Information Technology Laboratory-led programs and efforts by other agencies to respond to the manufacturing industry's need for safe, secure, reliable manufacturing systems and for predictable, well-characterized manufacturing processes and equipment.



NIST Industrial Control Security Testbed

Securing industrial control systems and networks is a challenge because they often work under real-time constraints that render standard IT security technology inapplicable. It can be difficult to balance performance, reliability, flexibility, safety and security. Safe operation is the number one concern and security requirements cannot compromise the safety requirements of the system. It is also difficult to specify requirements and testing capabilities of complex systems in operational environments. Devising technically sound industrial control system cyber security standards that gain global acceptance is also difficult because stakeholders – industry, government, standards developers – do not always have

the same interests and may never have articulated their standards goals. Very few industrial sectors have undertaken efforts to develop and implement a strategic, industry-wide approach to industrial control system cyber security. NIST works cooperatively with ICS communities in the public and private sectors to develop specific guidance on the application of the security controls, gathering relevant material from a variety of sources, analyzing it, and organizing it for easy adoption by industry.

Accomplishments:

- NIST SP 800-53 *Recommended Security Controls for Federal Information System*, Rev 2 is now a security standard that addresses both general Information Technology (IT) systems as well as ICS. An additional guidance document, NIST SP 800-82 *Guide to Industrial Control Systems (ICS) Security,* was developed to provide technical guidance for the public and private sectors on how to secure ICS while addressing their unique performance, reliability and safety requirements. NIST SP 800-82 has been downloaded over 350,000 times since the initial release and is heavily referenced by the industrial control community. A likely impact will be the voluntary adoption of the same or similar security requirements and baseline security safeguards and countermeasures by the private sector industrial control community.
- NIST delivered the "EtherNet/IP Performance Test Tool" to the Open DeviceNet Vendor Association (ODVA) on December 31st, 2007. This tool helps vendors test the performance and interoperability of their Ethernet/IP devices for industrial systems. It came about through an 18-month Cooperative Research and Development Agreement (CRADA) between NIST and ODVA, and was the highest priority task of the USCAR Plant Floor Controllers Task Force. ISD ran performance testing at six Plug-Fests since 2005. The Plugfests provide manufacturers a place to test the performance and interoperability of their Ethernet/IP devices for industrial systems.
- NIST technical leadership within the Department of Homeland Security (DHS) Control Systems Security Program helped produce a harmonized Catalog of Security Requirements that will facilitate [the development and convergence of control system cyber security standards applicable to the Critical Infrastructures and Key Resources (CI/KR) of the United States and other nations. This Catalog of Security Requirements is being actively vetted within the ISA SP99 WG4 (Technical Requirements for Industrial Automation and Control Systems (Part 4 Standard)) and IEC TC65/WG10 (Security for industrial process measurement and control - Network and system security) standards committees.

Future Directions and Plans:

Future efforts will expand industrial performance tests and will work within the numerous related standards organizations to achieve harmonization and increase speed and breadth of adoption by the manufacturing sector and other industries. The MEL-funded work will continue to leverage results from related projects funded by the Department of Homeland Security and the Department of Energy.

Planned future accomplishments:

- ISA SP99 Part 2 *Establishing an Industrial Automation and Control System Security Program* (Q2/FY08)
- Final SP 800-82 *Guide to Industrial Control System (ICS) Security* (Q4/FY08)
- First public draft of SP 800-53A *Guide for Assessing the Security Controls in Federal Information Systems* to address ICS (FY09)
- ISA SP99 Part 3 *Operating an Industrial Automation and Control System Security Program* (FY09 – FY10)
- ISA SP99 Part 4 *Technical Security Requirements for an Industrial Automation and Control System* (FY09 – FY10)
- Prototype development of the EtherNet/IP Performance Test Laboratory (Q4/FY08)
- Plug-Fest #8, Plug-Fest #9, Plug-Fest #10 (FY08 – FY09)
- Develop the capability to conduct performance tests on other industrial Ethernet-based networks (FY09-FY10)
- Expand the current performance test lab to include other industrial network types and technologies, including wireless and OPC (FY11 – FY12)

Collaborators and customers

- Bonneville Power Administration, Portland, OR
- Bureau of Reclamation, Washington, DC
- Department of Homeland Security, Washington, DC
- Federal Aviation Administration, Washington, DC
- Federal Energy Regulatory Commission, Washington, DC
- ISA, Research Triangle Park, NC
- ODVA, Ann Arbor, MI
- Tennessee Valley Authority, Knoxville, TN
- United States Council for Automotive Research, Detroit, MI
- Western Area Power Administration, Lakewood, CO

Awards and Recognition

Board Membership

Staff	Board Membership
Jim Gilsinn	• Director, Instrumentation, Systems, and Automation (ISA) society's Standards & Practices (S&P) Board

Leadership

Staff	Leadership
Jim Gilsinn	• Editor, ISA SP99 Committee on Security for Industrial Automation & Controls Systems, Working Group 2 • Coordinator, Open DeviceNet Vendor Association (ODVA) EtherNet/IP Implementers Workshop • Leader, ODVA EtherNet/IP Performance Workgroup • Leadership committee, ISA 99
Keith Stouffer	• Coordinator, NIST Federal Industrial Control System Security Workshop, NIST, April 2006 • Coordinator, 2nd Federal Industrial Control System Security Workshop, NIST, March 2007 • Chair, NIST Process Control Security Requirements Forum (PCSRF) • Technical Advisor, US TAG for the IEC TC65 committee • Leadership committee, ISA 99 • Technical Advisor, CIGRE B5 committee • Technical Advisor, DHS Control System Security Program

Excellence

Staff	Excellence Recognized
Joseph A. Falco Frederick Proctor Keith Stouffer Albert Wavering	• Department of Commerce Gold Medal for Distinguished Service (2005): For technical leadership of the NIST Process Control Security Requirements Forum culminating in the development of a common set of information security requirements for SCADA and industrial control systems used throughout the nation's critical infrastructure.
Keith Stouffer	• Invited speaker at over 25 international conferences and forums
Jim Gilsinn	• Senior Member, ISA society • 2006 ISA Standards & Practices Department Award