MEASURING IMPACT OF CYBERSECURITY ON THE PERFORMANCE OF INDUSTRIAL CONTROL SYSTEMS

BY KEITH STOUFFER AND RICK CANDELL, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Industrial control systems (ICS) are everywhere in our engineered world. They regulate temperature, lighting and access in our buildings; they provide fuel efficiency and safety while reducing emissions in our cars; they synchronize and regulate every aspect of production in our manufacturing plants; they monitor patients in our hospitals. In many cases the reliable and secure operation of such systems is essential, and they must be designed to be secure against hackers and terrorists. The National Institute of Standards and Technology (NIST) is developing a cybersecurity testbed for ICS. The goal of the testbed is to measure the performance of ICS when instrumented with cybersecurity countermeasures in accordance with practices prescribed by national and international standards and guidelines. Examples of such standards and guidelines include the ISA/IEC 62443 *Industrial Automation and Control Systems (IACS) Security* series of standards and NIST SP800-82, *Guide to Industrial Control Systems (ICS) Security*. The testbed will cover multiple types of ICS scenarios. Each scenario is intended to cover one or more aspects of industrial control.

ICS OVERVIEW

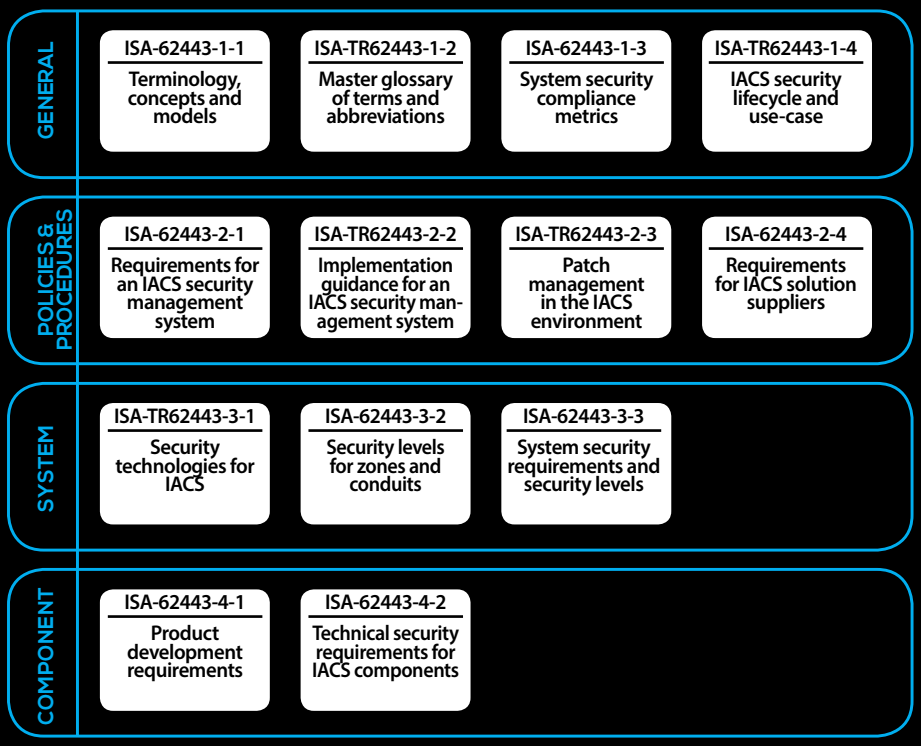
ICS is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and in critical infrastructures, such as industrial plants, water treatment facilities, power generation and distribution systems. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy) [1]. These types of networks are often composed of numerous interconnected devices with centralized or decentralized control depending on the application.

Modern requirements of modularity, decentralization, ease of maintenance, and lower operational costs have driven designers of ICS toward the adoption of Internet protocol (IP) routable data communications protocols traditionally found in home and office environments. With this change, ICS cybersecurity has become increasingly important. Traditional information technology (IT) security policies focus primarily on confidentiality with availability typically being the lowest security priority. In contrast, ICS, especially those considered critical infrastructure, must maintain a high level of system availability, data integrity and operational resilience for many reasons including economic, environmental, human safety, and national security. For many processes, it would be unacceptable to degrade ICS performance for the sake of security. A risk analysis is required for each system to make such a determination. Security countermeasures must be implemented in a way that maintains system integrity during normal operation as well as during a cyber-attack [3]. ICS security may include elements of resilient physical design (redundancy and physical adaptability) in addition to information security, to maintain acceptable system availability. Such requirements are determined by a process of careful risk analysis and system engineering [1]. The ICS cybersecurity testbed will serve as a test platform to provide guidance to the ICS community on implementing an ICS security program based on sound measurement science and standards.

TESTBED GOALS

The primary goal of the testbed is to measure the performance of ICS when instrumented with cybersecurity countermeasures in accordance with practices prescribed by national and international standards and guidelines. The results of this research will allow NIST to provide guidance to the ICS community on best practices for effectively implementing cybersecurity standards and guidelines without negatively impacting ICS performance. The testbed will be used to demonstrate the application of ICS cybersecurity standards such as the ISA/IEC 62443 [2] series, shown in Fig. 1, and NIST SP 800-82 [1],

FIGURE 1. ISA/IEC 62443 Series of Standards



to networked control systems, and measure the change in performance, if any, after applying security countermeasures. Some research areas of interest for the testbed include: perimeter network security; host-based security; user and device authentication; packet integrity and authentication; encryption; zone-based security; field bus (non-routable) protocol security; and robust/ fault tolerant control.

The secondary objective of the testbed is to measure the performance of ICS when under cyber-attack and secured with standards and guidelines as written. Resiliency will be a central research focus for systems under attack. Penetration testing will be conducted during the latter years of the ICS security research project; however, that timeline can be accelerated depending on the level of industry demand for penetration research. The results of this research will be fed back into the standards developing organizations for potential revision of the standards to address identified vulnerabilities, if any.

TESTBED DESIGN

The ICS cybersecurity testbed will be designed to demonstrate application of security countermeasures to a variety of processes such as control of a chemical plant, dynamic assembly using robots, additive manufacturing, and supervision and control of large distributed networks such as intelligent transportation systems. Each scenario is intended to cover one or more aspects of industrial design. The Tennessee Eastman scenario defined by Downs and Vogel [4] is intended to cover continuous process control. A collaborative robotic assembly scenario is intended to cover rapid and dynamic discrete manufacturing. An additive manufacturing scenario is intended to cover advanced manufacturing processes, and an intelligent transportation scenario is intended to cover large distributed networks for industrial systems such as railways and pipelines involving SCADA systems.

While it is not practical to construct an entire industrial operation such as chemical process control within the laboratory, simulation and emulation will be leveraged where appropriate with hardware-in-the-loop (HIL) components simulating real-world interfaces between the sensors and actuators and the controller.

MEASUREMENT APPROACH

A measurement enclave will be constructed within the testbed to capture network traffic, retain system log messages, and manipulate traffic. Traffic manipulation will be used for man-in-the-middle attacks, traffic shaping, and local and wide area network modeling.

The testbed is designed to support three measurement approaches. The first measurement approach will be to introduce communication link uncertainty between sensors and controllers. ICS process performance will be measured and correlated with varying degrees of channel degradation. This approach will provide a technology-independent view of how processes are impacted by certain channel models indicative of security countermeasures.

The second approach will be to demonstrate the process for developing a risk model and applying cybersecurity countermeasures in accordance with ISA/IEC 62443 and NIST SP 800-82. This approach will demonstrate how to apply the standards with multiple levels of security to industrial processes. For each scenario (i.e., process and security level), the performance of the system will be measured with and without the security countermeasures in place to provide a comparison of performance of a system instrumented with security but not undergoing attack.

For the third approach, the performance of the system will be measured while under cyber-attack. For each process undergoing evaluation, test scenarios will entail multiple levels of security.

FIGURE 2. Collaborative Robotic Assembly Scenario in NIST ICS Cybersecurity Testbed

INDUSTRIAL SCENARIOS

In December 2013, NIST sponsored a 2-day roadmapping workshop on measuring the impact of cybersecurity on ICS performance. At this workshop, attendees from industry, academia, and government were asked to participate in defining the priorities of the testbed. In particular, the protocols identified for inclusion in the testbed were primarily IP-routable protocols. Non-routable protocols were indicated to be of lesser importance. For inclusiveness, the ICS cybersecurity testbed will include both types of protocols.

Chemical Process Control

The Tennessee Eastman (TE) model was chosen for the chemical process control scenario for several reasons. First, the TE model is a well-known plant model used in control systems research and the dynamics of the plant process are well-understood. Second, the process must be controlled; otherwise perturbations will drive the system into an unstable state. By being open-loop unstable, the TE process model represents a real-world scenario in which a cyber-attack could pose a risk to human safety, environmental safety, and economic viability. Third, the process is complex, highly non-linear, and has many degrees of freedom by which to control and perturb the dynamics of the process. And finally, numerous simulations of the TE process have been developed and reusable code is readily available. The University of Washington Simulink controller model by Ricker [5] was chosen for its multi-loop control

ABOUT THE AUTHORS

Keith Stouffer has been with the Engineering Lab at NIST for 25 years focusing on ICS security since 2000. Mr. Stouffer is the lead author of NIST Special Publication 800-82, Guide to Industrial Control Systems Security, which provides guidance on how to secure ICS while addressing their unique performance, reliability and safety requirements. Mr. Stouffer has also provided input to the ISA/IEC 62443 and NERC CIP security standards. During his career, he has received Gold and Bronze Medals from the Department of Commerce and the Gov30 Security Award. Mr. Stouffer holds a Master's degree in Computer Science from Johns Hopkins University and a Bachelor's degree in Mechanical Engineering from the University of Maryland.

Keith Stouffer and Rick Candell

Rick Candell has twenty years of experience in telecommunications with emphasis on tactical radio and satellite-based tracking systems. Mr. Candell spent twelve years developing, testing, and deploying secure wireless technologies for the US Army. He was an important contributor in developing cost-saving technologies for the US Army fleet tracking system. He holds patents related to successive interference cancellation and transmission burst detection. Mr. Candell recently joined the NIST Engineering Laboratory where he is applying his wireless networking and information security knowledge to industrial control systems. Mr. Candell holds an MSEE degree from the University of Memphis.

architecture making distributed control architectures viable. The TE process will be controlled by real ICS hardware and software.

Other chemical processes being considered for the simulator include a dynamic model of a benchmark manufacturing process used to produce vinyl acetate (VAC) monomer [6]. The process shares many performance metrics and security vulnerabilities with the TE process while highlighting some key differences that warrant investigation from a cybersecurity perspective. The VAC process model is significantly larger in terms of interacting modules and dynamic states. The VAC process features 246 states, 26 manipulated variables, and 23 polled measurements, as opposed to 50 states, 12 manipulated variables, and 22 polled measurements for the TE process. The process is controlled using a multiloop Single Input Single Output architecture, which lends itself to more granular evaluation of targeted control system vulnerabilities. The process features multiple vapor phase reactions with much faster dynamics requiring a 1 second sampling interval, while the sampling interval for the TE process is 40 seconds. The faster sampling interval makes the system especially sensitive to delays in communication and loss of synchronization across independent control loops.

Collaborative Robotic Assembly

The collaborative robotic assembly scenario, shown in Fig. 2, will be used to demonstrate cybersecurity application in a discrete state process with fast dynamics and high data throughput demands using a combination of a deterministic real-time protocol and an Ethernet-based IP protocol. The collaborative robotic assembly system will demonstrate the impacts of cybersecurity on a system with embedded control and dynamic planning. The collaborative robotics scenario will be constructed as multiple local area networks with EtherCAT serving as a real-time conduit between sensors, controllers, robots, and a safety system.

A safety system will be constructed to measure performance of ICS safety systems when instrumented with cybersecurity countermeasures. The safety system will include a safety PLC, an emergency stop button, a solid state relay, and a light curtain sensor. The safety PLC will be networked to the main robot controller using the real-time EtherCAT bus as well as the non-real-time Ethernet interfaces.

Additive Manufacturing

The additive manufacturing scenario is intended to cover advanced manufacturing processes. Additive manufacturing is rapidly evolving from just a prototyping tool to a production method for functional parts. The ability to produce small quantities efficiently makes it particularly attractive. Information about materials, finish, and other physical attributes are all contained in the digital production (print) file, which makes this file a critical piece of intellectual property to protect. The testbed currently contains a networked extrusion type 3D printer for cybersecurity testing.

Intelligent Transportation

The intelligent transportation scenario is intended to cover large distributed networks for industrial systems such as SCADA systems. The specific system to be simulated has not yet been selected, but candidate systems include railway and an intelligent transportation system for a large metropolitan area. Cybersecurity for single-hop and multi-hop wireless architectures will be explored within this scenario.

DISCLAIMER

Certain commercial equipment, instruments, or materials may be identified in this article in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

CONCLUSION

Control systems are embedded in essentially all engineered systems, such as our cars, homes, offices, industrial plants, and in critical infrastructures such as power plants, water treatment plants, and transportation systems. To ensure the security of industrial control systems (ICS), particularly for critical infrastructures, standards are being developed to ensure ICS cybersecurity. The NIST ICS cybersecurity testbed will be constructed to facilitate the measurement of industrial process performance for systems instrumented with cybersecurity technologies. This testbed will allow for validation of existing security standards and guidelines and will allow researchers to provide valuable feedback to the community on methods, practices, and pitfalls when applying a cybersecurity program to an ICS. Additional work will be required to identify new use cases and pertinent performance metrics. The testbed will provide an opportunity for collaboration between government, research institutions, and industry partners. Interested parties are encouraged to contact the authors directly to discuss opportunities for collaboration. ■

REFERENCES

1 Keith Stouffer, Joe Falco, and Karen Scarfone, "Guide to Industrial Control Systems (ICS) Security," National Institute of Standards and Technology, Special Publication 800-82, Revision 1, 2013.

2 "Industrial Automation and Control Systems Security," ANSI/ISA-62443, 2007-2013.

3 Eric Knapp, *Industrial Network Security Securing Critical Infrastructure for Smart Grid, SCADA, and Other Industrial Control Systems.* Waltham, MA: Syngress, 2011.

4 J.J. Downs and E.F. Vogel, "A Plant-Wide Industrial Process Control Problem," *Computers and Chemical Engineering*, vol. 17, no. 3, pp. 245-255, 1993.

5 N. Lawrence Ricker. (2002, December) New Simulink models of two decentralized control strategies. http://depts.washington.edu/control/LARRY/TE/download.html#Multiloop

6 Michael L. Luyben and Björn D. Tyréus, "An industrial design/control study for the vinyl acetate monomer process," *Computers & Chemical Engineering*, vol. 22, no. 7, pp. 867-877, 1998.