ISA Process Control & Safety Symposium2014
6–9 October 2014
Houston Marriott West Loop by the Galleria
Houston, Texas USA

A Cybersecurity Testbed for Industrial Control Systems

R. Candell, D.M. Anand, and K. Stouffer

National Institute of Standards and Technology, Gaithersburg MD, U.S.A
[rick.candell, dhananjay.anand, keith.stouffer]@nist.gov

Abstract — The National Institute of Standards and Technology (NIST) is developing a cybersecurity testbed for industrial control systems (ICS). The goal of this testbed is to measure the performance of an ICS when instrumented with cybersecurity protections in accordance with practices prescribed by prevailing standards and guidelines. This paper outlines the testbed design and lists research goals, use cases, and performance metrics currently being considered. The paper is also intended to initiate discussion between control and security practitioners – two groups that have had little interaction in the past. Research outcomes from the testbed will highlight specific cases where security technologies impact control performance, as well as motivate methods by which control engineers can leverage security engineering to design control algorithms that extend safety and fault tolerance to include advanced persistent threats.

Keywords — industrial control systems, robotics, chemical process control, cybersecurity, industrial security, process resilience, penetration testing, process performance, measurement science, testbed, robotics, robot control, safety, supervisory control and data acquisition (SCADA)

I. Introduction

Given the increasing interest in security of industrial control systems (ICS) and the evolving nature of advanced persistent threats against critical industrial infrastructure [1], the National Institute of Standards and Technology (NIST) has been actively involved in developing standards for cyber and control systems security via several standards bodies. Examples of such standards and guidelines include [2] and [3]. A research testbed, currently in development at NIST, will provide a platform on which to apply cybersecurity strategies to use cases that are practically relevant to industry.

Industrial control system (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 critical infrastructures. 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) [2]. 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 network control systems toward the adoption of Internet protocol (IP) routable data communications protocols traditionally found in home and office environments.

With this change ICS security has become increasingly important. Traditional information technology (IT) security policies focus primarily on confidentiality with network availability being the lowest security priority. In contrast, ICSs, especially those considered critical infrastructure, must maintain a high level of system availability and operational resilience for many reasons including economic, environmental, human safety, and national security. For many processes, it would be unacceptable to degrade performance for the sake of security. A risk analysis is required for each system to make such a determination. Security protections must be implemented in a way that maintains system integrity during normal operation as well as during times of cyber-attack [4]. Indeed, ICS security must include elements of resilient physical design (redundancy and physical adaptability) in additional to network security to maintain acceptable system availability. Such requirements are determined by a process of careful risk analysis and system engineering [2]. The ICS testbed will serve as a test platform to provide guidance to the ICS community on how to implement an ICS security program based on sound measurement science. This paper describes our objectives and our approach to developing ICS scenarios for the purpose of measuring system performance. Feedback from industry and academia is encouraged and appreciated.

II. Objectives

The primary goal of the testbed is to provide guidance to industry on the best practices for implementing cybersecurity strategies within an ICS. The ICS cybersecurity testbed will be designed to demonstrate application of security to a variety of processes such as control of a chemical plant, dynamic assembly using robots, and distributed supervision and control of large wide area networks such as gas pipelines, water distribution pipelines, and intelligent transportation systems. As stated, the primary objective of the testbed is to demonstrate the application of industrial control system security standards such as ISA/IEC-62443[1] to a networked control system and measure the performance degradation or improvement, if any, after applying security protections. Through the rigorous measurement science, the testbed will demonstrate the impacts of cybersecurity on the performance of industrial control systems and serve as a guide on how to implement security safeguards effectively without negatively affecting process performance. While no system can be made completely secure from network attack [5], a

[1] The International Society of Automation (ISA) originated a set of standards referred to as ISA99. ISA later renumbered the series to align with the International Electrotechnical Commission (IEC) format.

secondary objective of the testbed is to measure the performance of ICS while undergoing cyber-attack. Resiliency will be a central research focus for systems under attack. The testbed will support research for a period of at least five years. 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.

III. Testbed Design Approach

The design of our ICS cybersecurity testbed will cover multiple types of ICS scenarios. Each scenario is intended to cover one or more aspects of industrial design. The Tennessee Eastman scenario defined by Downs and Vogel [6] is intended to cover continuous process control. The robotic assembly scenario is intended to cover rapid and dynamic discrete manufacturing. An additional enclave which will be selected at a later date is intended to cover wide area industrial networks (WANs) for systems such as pipelines and railroads involving a safety-critical supervisory control and data acquisition (SCADA) solution.

Our testbed network configuration is shown in Figure 1. Each ICS scenario will be allocated to an "enclave" within the testbed, and each enclave will be logically separated from the other enclaves. A demilitarized zone (DMZ) will be constructed to host an enterprise historian and other services that are usually accessible by enterprise network users and plant operators. A measurement enclave will be constructed to capture network traffic, retain *syslog* messages, and manipulate traffic. Traffic manipulation will be used for man-in-the-middle attacks; traffic shaping; and local and wide area network modeling. Where local switching devices are employed, port mirroring will be used to send packets to the measurement enclave. This is a common approach to network traffic capture that will be useful for collecting data for offline analysis.

Security devices will be deployed throughout the network. Firewalls will have the capability to perform device authentication, encryption, and deep packet inspection. Security devices will be used to demonstrate resilience and allow researchers to measure performance of processes under varying levels of security. Our approach to measuring the performance impact of security will require the introduction of varying degrees of packet flight time uncertainty (delay and jitter) and packet loss. Performance of the network will be analyzed as a function of these parameters. Statistical metrics collected by this approach will provide design guidance to component manufacturers and system integrators on how security impacts determinism, safety, and stability. Performance metrics are discussed in the section on Metrics.

IV. Measurement Approach

The testbed is designed to support three measurement approaches. The first measurement approach will be to introduce communication link uncertainty between sensors and controller. 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 counter-measures.

The second approach will be to demonstrate the process for developing a risk model and applying cybersecurity countermeasures in accordance with ISA/IEC-62443 [3] Parts 3-1 through 3-3 and NIST SP 800-82 [2]. This approach will demonstrate how to apply the standard with increasing levels of security to real-world processes. For each scenario (i.e., process and security level), we will measure the process performance of the system with and without the security countermeasures to provide a comparison of performance of a system instrumented with security but not undergoing attack.

For the third approach, we will measure process performance while the process undergoes cyber-attack. Tools such as Metasploit[2] will be used [7]. For each process undergoing evaluation, test scenarios will entail an increasing level of security. For each test scenario, we will evaluate process performance metrics defined in section VII.

V. Application Scenarios

NIST sponsored a road-mapping workshop in December 2013. At this workshop, industry and academia 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. Other "field-bus" protocols such as those based on the controller area network (CAN) were indicated to be of lesser importance. For inclusiveness, our testbed includes both types of protocols; however, IP-routable protocols will be favored.

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

A. Chemical Process Control

The Tennessee Eastman (TE) model was chosen for a number of 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 an appreciable 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. We chose the University of Washington Simulink controller model by Ricker [8]. The Ricker Simulink model was chosen for its multi-loop control architecture making distributed control architectures viable.

[2] Refer to paragraph Disclaimer

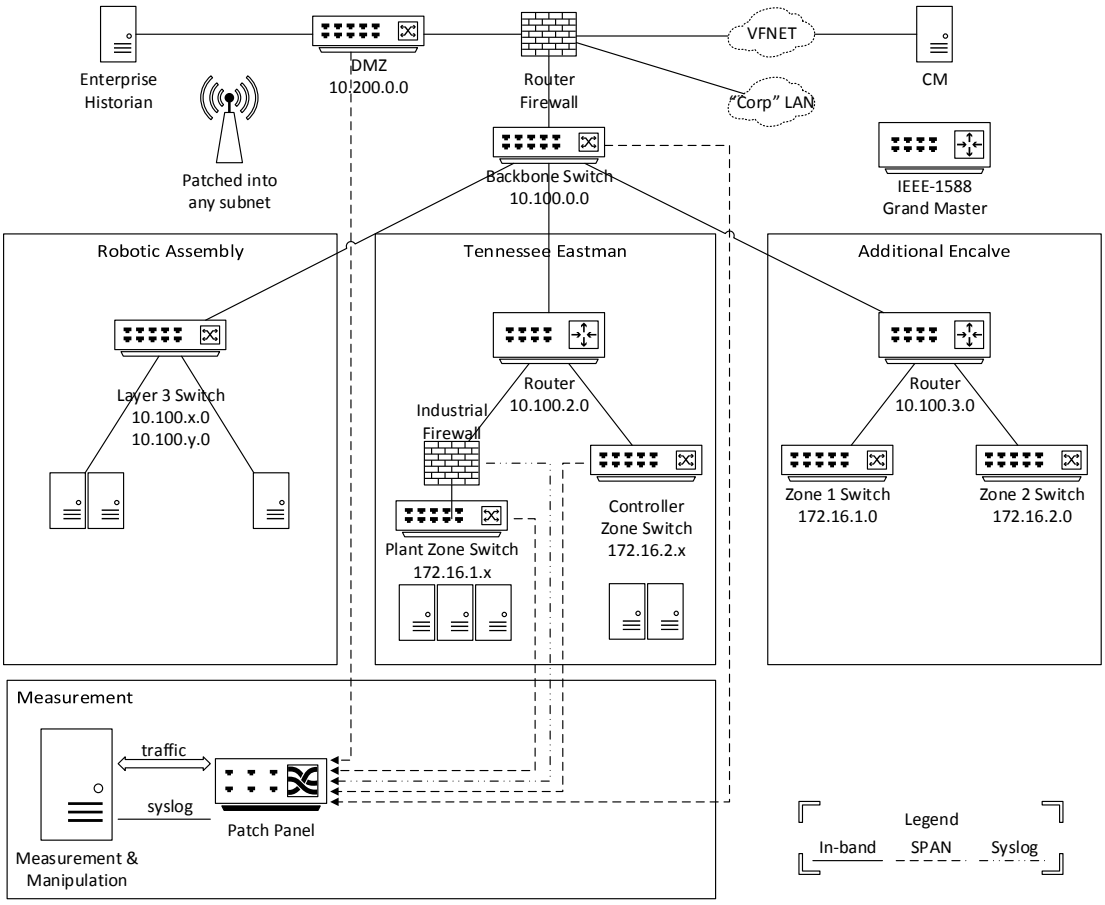

Figure 1. Testbed Network Design

The TE process model is illustrated in Figure 2. Downs and Vogel did not reveal the actual substances used in the process, but instead used generic identifiers for each. The process produces two products, G and H from four reactants A, C, D, and E. The process is defined as irreversible and exothermic, and the reaction rates of the four reactants are a function of the reactor temperature. The process is broken into five major operations which include a reactor, a product condenser, a vapor-liquid separator, a product stripper, and a recycle compressor.

The process is described in detail in [6], however a synopsis is given as follows. Gaseous reactants are combined in the reactor to form liquid products. The reactor temperature must be controlled and is cooled using cold water cooling bundles. The reaction is not 100 % efficient and some gaseous feed components remain. The output of the reactor is fed to a condenser where the products are further cooled into liquid form. The vapor-liquid separator then separates unreacted gases from the liquid products. The unreacted gases are sent back to the reactor by a centrifugal recycle compressor. Again,

the separate process is not 100 % efficient, and the remaining reactants are removed in a stripping column by stripping the mixture with C in feed stream four (4). The products, G and H, are then sent downstream for further refining. Byproducts of the process are purged from the process through the purge valve of stream nine (9).

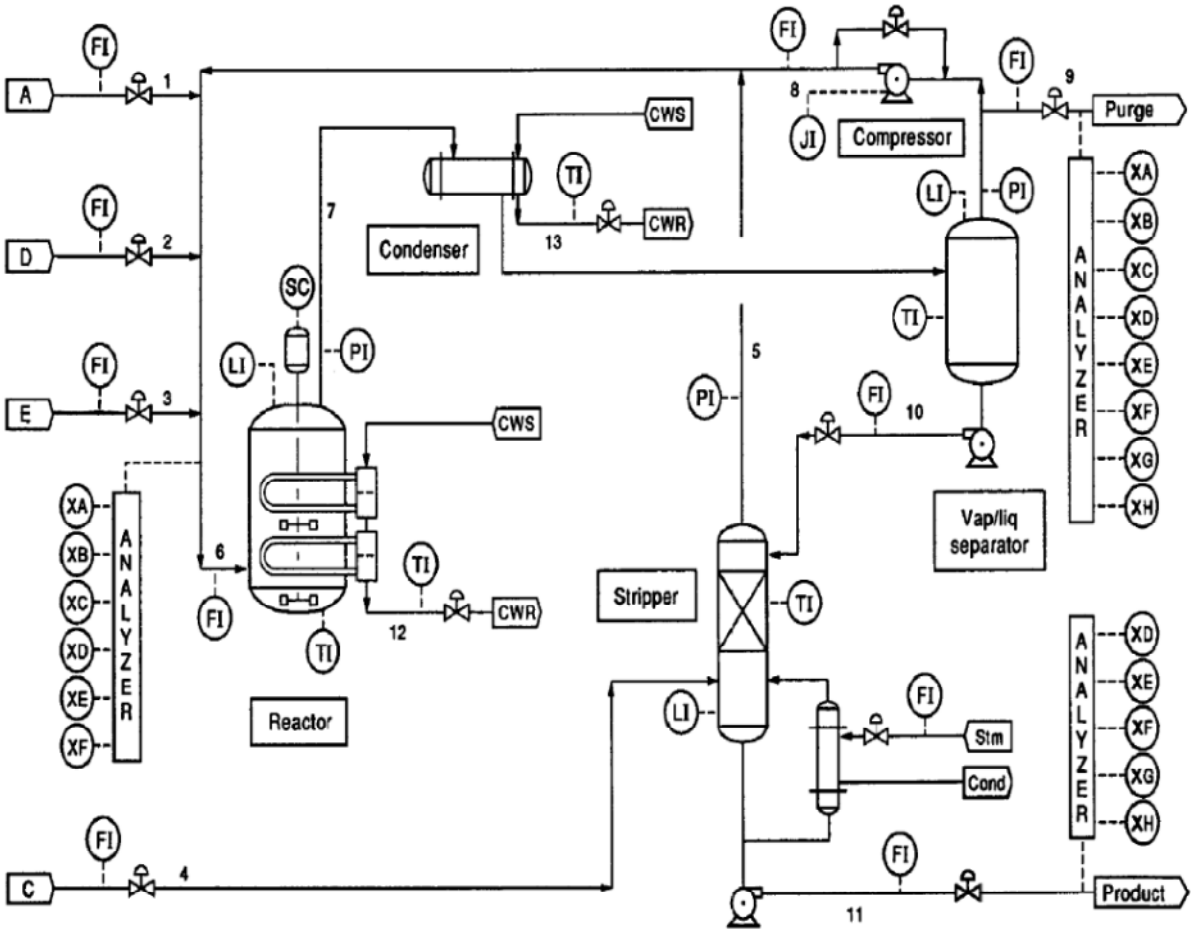

Figure 2. Tennessee Eastman Control Problem

The process has six (6) different modes of operation which control the G/H mass ratio and the production rate through stream eleven (11). Our primary use case for the system will be the base case indicated as Mode 1. Downs and Vogel provided heat and material balance data for the Mode 1 case. It is important to note that the process is designed to shut down if the reactor pressure exceeds 3000 kPa; however, as noted in [5] the reaction efficiency improves as reactor pressure increases. This indicates that reactor pressure must be driven as close to the maximum threshold without exceeding the shutoff limit. The reactor pressure therefore represents a security vulnerability. It is conceivable that an attacker could target the reactor pressure using a geometric attack or a surge attack combined with a human-machine interface (HMI) spoofing attack. Krotofil and Cardenas provide an excellent discussion of the TE process and potential security vulnerabilities [9].

The controller is implemented entirely in Simulink, and the plant uses an S-function implementation written in M. The plant and controller have been separated such that the two processes may be placed on separate machines with communications conducted via an arbitrary network connection. Structured industrial protocols will be used as application layer interconnects between the plant and the controller.

For an analog analysis of performance, a network connection is unnecessary, and instead a channel model may be inserted to simulate the effects of the communication link. The channel model will simulate packet error rate and delay variation of the communications links between sensors/actuators and the controller. Using this approach we will predict in simulation the effect of the cybersecurity on the performance of the control system.

While a mathematical simulation is an important first step in the analysis of the performance of any system, it will be equally important to understand how a practical system behaves when instrumented with security protections that will invariably insert packet flight uncertainties. A hardware-in-the-loop (HIL) simulator will therefore be constructed to demonstrate the impacts of cybersecurity on the performance of a manufacturing process. The HIL simulator will also serve as a performance measurement platform for other processes.

The simulator is intended to be reconfigurable such that various network topologies and processes may be hosted and evaluated. For the TE process the enclave will be partitioned in accordance with the baseline case shown in Figure 3.

The system will be broken into a plant zone, a control zone, and a demilitarized zone. The plant zone will host the TE plant process. State data in the plant process will be communicated to a programmable logic controller (PLC) using one or more industrial protocols such as the non-IP-routable protocol, DeviceNet, and the IP-routable protocol, EtherNet/IP. In the baseline scenario, the PLC will be used to store the state data in an Open Platform Communications (OPC) server. A local historian will be used to record the state data and replicate that data to an enterprise historian in the DMZ.

The controller process will be hosted in the control zone. The control zone will be configured in a separate subnet from the plant zone. The controller process will be implemented in Simulink, and the MATLAB OPC Toolbox will be used to read and write state data to the OPC server. Control actuation will be triggered when the controller writes data to the OPC server. The OPC server will update the PLC state with the actuator command which will in turn produce a state change in the plant process. Using OPC in this way will demonstrate process control using multiple subnets and a centralized industrial data server. A firewall with deep packet inspection and device authentication (white listing) will be inserted as a PLC cyber-protection mechanism.

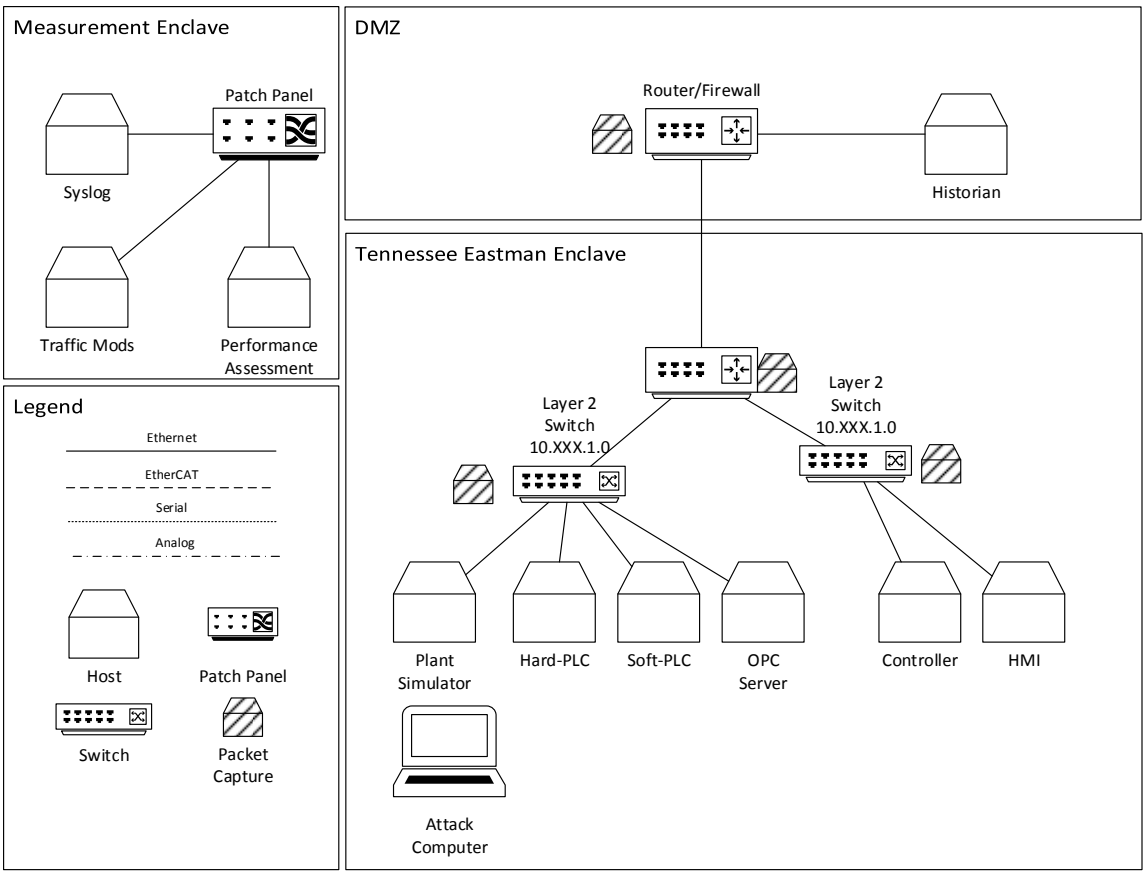

Figure 3. TE Process Enclave Network Diagram

As stated above, the HIL simulator is intended to be a flexible platform that may be easily reconfigured or repurposed. Additional use cases for the TE simulator include:

- Partitioning of the industrial network into different network topologies;
- Introduction of a personal computer (PC)-based PLC as the control platform to allow for cybersecurity technologies to be applied at the host level;
- Use of direct EtherNet/IP communication between the controller and the sensor actuators implemented using standard personal computers; and
- Implementation of other manufacturing processes with faster dynamics.

The TE enclave will be connected to the measurement zone for packet capture and the implementation of custom channel models that will serve to emulate the delays and bandwidth constraints introduced by security devices.

Other chemical processes being considered for the simulator include a dynamic model of a benchmark manufacturing process used to produce Vinyl Acetate (VAC) monomer [10]. The process shares many performance metrics and security vulnerabilities with the TE process while highlighting some key differences that warrant investigation from a security perspective. Firstly, 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 multi-loop Single Input Single Output architecture, which lends itself to more granular evaluation of targeted control system vulnerabilities. Finally, 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. A publicly available MATLAB model of the VAC process has been made available in [11].

B. Collaborative Robotic Assembly

The robotic assembly enclave 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 robotic assembly system will demonstrate the impacts of cybersecurity on a system with embedded control and dynamic planning. The robotics enclave network design is shown in Figure 4. The robotics enclave will be constructed as multiple local area networks with EtherCAT serving as a real-time conduit between sensors, controller, robots, and a safety PLC. The robotics enclave will not be a simulation.

The robotics enclave will be constructed similar to the TE Enclave such that different functions of the robotics system will be encapsulated in more one than one subnet. A layer 3 switch will be used to facilitate rapid network reconfigurability; and, similar to the TE enclave, the robotics enclave will serve to validate the requirements specified in ISA/IEC-62443-3-3.

A safety circuit will be constructed to measure stopping performance of a control system instrumented with cybersecurity protections. The safety circuit 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.

The measurement enclave will be used to simulate communication channel degradation in the form of packet loss, packet manipulation, and flight time uncertainty. Stop-time performance of the safety circuit will be measured as a function of the security technologies used or the channel model employed depending on the test scenario.

C. Wide-area Network Control System

A third enclave is envisioned for the testbed. This enclave will be directed toward security of wide-area SCADA networks. The specific system to be simulated has not yet been selected, but candidate systems include an intelligent transportation system for a large metropolitan area or a pipeline with rotating machines and many sensors covering a large geographical area. Single-hop and multi-hop wireless architectures will be explored within the third enclave.

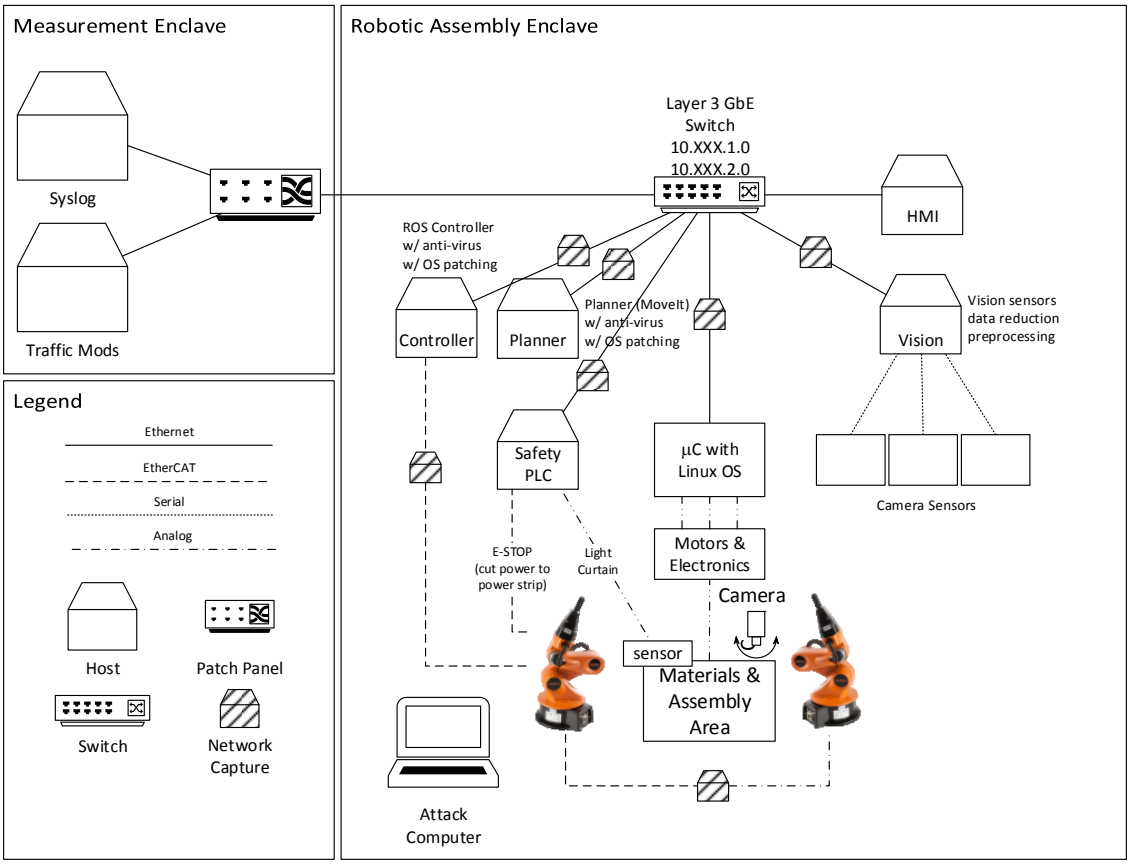

Figure 4. Robotic Assembly System Network Diagram

VI. Security

Our testbed is designed for measuring industrial process performance of systems with installed security measures. This testbed will focus on the impact of security technologies. Security technologies may be classified as perimeter-based and host-based technologies. Technologies such as power finger-printing and radio frequency finger-printing are considered host-based technologies. Security technologies will be selected in accordance with their anticipated impact on process performance.

ISA/IEC-62443 Part 3-3 *System security requirements and security levels* lists the requirements that system integrators should take to safeguard their operation. The complete list of the requirements is too extensive to reproduce here; however, it is important to understand that the requirements listed in the standard impact the security countermeasures that will be used to protect an operation. ISA/IEC-62443 Part 3-2: *Security risk assessment and system design* explains the steps required to perform a high level risk assessment and how to partition the ICS operation into zones and conduits. The ISA/IEC-62443-3-1 working draft identifies technologies available to fulfill ICS cybersecurity requirements. As stated earlier, ISA/IEC-62443 parts 3-1 through 3-3 will be applied to each process as part of the second and third measurement approaches.

VII. Metrics

Rating the performance of an ICS is a challenging exercise. While industrial processes can be classified into general categories, no one set of metrics can be designed to cover all possible scenarios. Top level categories of processes include continuous processes, discrete processes, and a hybrid of continuous and discrete processes. Continuous processes are those in which materials flow through a system typical without pause or wait states. Discrete processes include those in which materials flow in quantized bundles and pauses or wait states are frequent. Many processes which appear to be mostly continuous are actually continuous processes with discrete elements and may be classified as hybrid processes. Process categories and examples of each are given in Table 1.

Table 1. Categories or Industrial Processes

Category	Examples of processes
Highly continuous process	Chemical manufacture Oil and Gas refineries Oil and Gas production and distribution Semiconductor manufacture Smelting Disinfection
Highly discrete process	Robotic sorting & assembly Automotive assembly Building automation
Hybrid	Pharmaceutical manufacture Metal-alloy manufacture

A one size fits all approach to a data-based assessment of performance of an ICS is very difficult and somewhat impractical. Much effort has been spent in identifying the technical indicators for assessing process performance. Both security metrics and process performance metrics exist and may be applied to industrial processes. Process performance metrics may include throughput, product quality, product error rate, and operational cost. Security metrics are defined for information technology in publications such as NIST SP 800-55 [12] and the *Common Criteria for Information Technology Security Evaluation (CC)* [13].

For the purpose of assessing the impact security has on process performance, it is necessary to measure the operational performance of the process. It makes little sense to measure security performance (i.e., effectiveness) without first understanding how security technologies impact the performance of the process being protected. Therefore, for the purpose of assessing process performance, our approach is to focus on the technical performance indicators of the processes rather than information security

metrics. Industrial metrics are listed in listed in Table 2 through Table 6. Metrics for continuous processes, discrete processes, computer system performance, and network performance are organized in separate tables.

Table 2. Dynamic Performance Metrics for Continuous Processes

Metric	Description
% Process Availability	The ratio of process up-time to the sum of process up-time and down-time
Product Quality	Statistical measures of product goodness or purity
Process Variability	Statistical measurement of how much a process variable deviates or oscillates from its steady state value or set point.[3]
Cost	The economic cost for running the process measured in currency
Safety Margin	Timeliness to shutdown process after fault detection. This may be particularly important where human safety is concerned.
% Time Actuation at Limits	Measure of the amount of time a process control variable remains at a hard limit. A common example of such a limit includes valves at full open or full close.
Integrated Absolute Error (IAE)	Commonly used metric for evaluating the performance of a feedback control loop. [14]
Integrated Time-weighted Absolute Error (ITAE)	Commonly used metric for evaluating the performance of a feedback control loop. This particular metric weights the steady state error more than the error introduced by the transient response. [14]

Table 3. Dynamic Performance Metrics for Discrete Processes

Metric	Description
Product Quality	A quantitative measurement of product goodness or purity
Defect Rate	Rate at which a product fails quality control checks due to errors in the manufacturing process.
Defects per unit	Statistical measures of the number of defects per unit
Process Restart Rate	Number of times a process must be restarted in a given time interval.
Variability of On-time Actuation	Statistical measure of time between command and actuation completion.

[3] Not all process state variables have pre-determined set points. Manual overrides are available in some control systems.

Metric	Description
Steady State Error	Oscillation over variability about a pre-determined set point.
Response Time	A quantitative measurement of time to respond to a perturbation such as a step stimulus.
Process Duration	Length of time to complete a sequence of tasks such as a series of assembly tasks in a robotic assembly system.

Table 4. Dynamic Metrics for Measuring System Performance

Metric	Description
Volatile Memory	Utilization of system memory typically reported as a percentage of total RAM
Non-volatile Memory	Utilization of system memory typically reported as a percentage of total system disk space
CPU Utilization	Percentage of the total CPU usage time
I/O Read Load	Total bytes read in the CPU I/O channel
I/O Write Load	Total bytes written in the CPU I/O channel
Missed Scans (Rate)	When using a device such as a PLC that scans all variables before executing the next iteration of control, the total number of sensor readings missed in a given time interval.

Table 5. Nominal System Properties for Measuring System Performance

Metric	Description
Medium Type	Examples include Copper, Fiber, Wireless and the associated protocol used such as CAT-6 copper or 802.11g wireless.
Physical Channel Bandwidth	The full bandwidth allocated to the channel. This can be useful for wireless channels such as IEEE 802.15.4 and modulated wired channels such as Ethernet.
Rated Channel Capacity	Rated capacity for transmitting and receiving elements in the network
Channel Encoding	Algorithm or structure used to encode the transmissions to include interleaving, channel coding, modulation, and interference handling properties
Environmental Characteristics	Mechanical, electrical, and electromagnetic properties of the environment in which the system is deployed.
Channel Compression	The data compression algorithm used for transmission
Rated Channel	The advertised theoretical throughput for a given

Metric	Description
Throughput	transmitting or receiving device
Routing Algorithms Used	The type of routing algorithm employed. Knowing the routing algorithm is particularly useful for mobile ad-hoc networks and fully loaded ad-hoc networks.
Switching Algorithms Used	The type of layer 2 switching algorithm employed.
Determinism Boundaries	Real-time constraints of the system which is known a *priori*

Table 6. Quantitative Dynamic Metrics for Measuring Network Performance

Metric	Description
Information Packet Rate	Rate of information packet flow that is useful to the application measured at the highest observable network layer.
Information Bit Rate	Rate of information bit flow that is useful to the application measured at the highest observable network layer.
Raw Packet Rate	Measured at layer 2 and includes overhead and retries
Raw Bit Rate	Measured at layer 2 and includes overhead and retries
Message Delay (Distribution)	The delay for full messages (multiple packets) to be propagated through the network or network link. Used for long packets measured at the layer in which transport layer packets are reassembled which is usually the application layer.
Packet Delay (Distribution)	The delay for single packets to be propagated through the network or network link.
Packet Delay Jitter	Variation in delay measured over an ensemble of packets.
Processing Delay	Delay introduced by network interconnect devices such as switches and routers
Queuing Delay	Amount of time a packet spending in the input queue before being processed
Propagation Delay	The amount of time a quanta of information takes to travel between transmitter and receiver[4]
Packet Collisions	Number of collisions typically reported by layer 2 devices
Packet error rate	Rate of packet errors measured at the transport layer

[4] This may be particularly useful for wireless channels such as low earth orbital and geostationary satellite links in which the distance between transmitter and receiver is large relative to the transmission speed of the medium.

Metric	Description
Packet loss rate	Rate of packet loss measured at the transport layer[5]
Packet Size (Distribution)	Distribution of the size of packets transmitted across the network.
Measured Determinism Boundaries	Measured points of real-time determinism failure

VIII. Conclusions

The NIST ICS cybersecurity testbed will be constructed to facilitate the measurement of industrial process performance indicators 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 industry on methods, practices, and pitfalls when applying a cybersecurity program to an industrial system. More work will be required to identify new use cases and pertinent performance metrics. We will continue to refine our technique for measuring ICS security performance, and our results will be reported in subsequent publications. This testbed will provide an opportunity for much needed collaboration between government, research institutions, and industry partners. Interested parties are encouraged to contact the authors directly to discuss opportunities for collaboration.

DISCLAIMER

Certain commercial equipment, instruments, or materials are identified in this paper 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.

REFERENCES

[1] "Computer Security Incident Handling Guide," NIST Special Publication 800-61, 2012.

[2] Keith Stouffer, Joe Falco, and Karen Scarfone, "Guide to Industrial Control Systems (ICS) Cybersecurity," National Institute of Standards and Technology, Special Publication 800-82, 2011.

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

[4] Eric Knapp, *Industrial Network Security Securing Critical Infrastructure for Smart*

[5] Packet loss occurs due to collisions for non-reliable protocols and queuing loss due to severe network congestion.

Grid, SCADA, and Other Industrial Control Systems. Waltham, MA: Syngress, 2011.

[5] Alvaro Cardenas et al., "Attacks Against Process Control Systems: Risk Assessment, Detection, and Response," in *ASIACCS 2011*, Hong Kong, China, 2011.

[6] 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.

[7] David Maynor, *Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research*.: Syngress, 2007.

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

[9] Marina Krotofil and Alvaro A. Cardenas, "Resilience of Process Control Systems to Cyber-Physical Attacks," in *NordSec 2013*, Ilulissat, Greenland, 2013.

[10] 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.

[11] Rong Chen, "A nonlinear dynamic model of a vinyl acetate process," *Industrial & engineering chemistry research*, vol. 42, no. 20, pp. 4478-4487, 2003.

[12] Elizabeth Chew et al., "Performance Measurement Guide for Information Security," NIST, Gaithersburg, Special Publication NIST SP-800-55, 2008.

[13] Common Criteria Recognition Arrangement (CCRA), Common Criteria for Information Technology Security Evaluation, 2012.

[14] Pau Marti, Josep Mª Fuertes, and Gerhard Fohler, "A control performance metric for real-time timing constraints," in *Proceedings of the 14th Euromicro International Conference on Real-Time Systems*, 2002.

[15] Feng-Li Lian, James R. Moyne, and Dawn M. Tilbury, "Performance Evaluation of Control Networks: Ethernet, ControlNet, DeviceNet," *Control Systems Magazine*, no. February, pp. 66-83, 2001.

[16] Daniel E. Rivera. Tennessee Eastman Problem for MATLAB. [Online]. http://csel.asu.edu/node/33