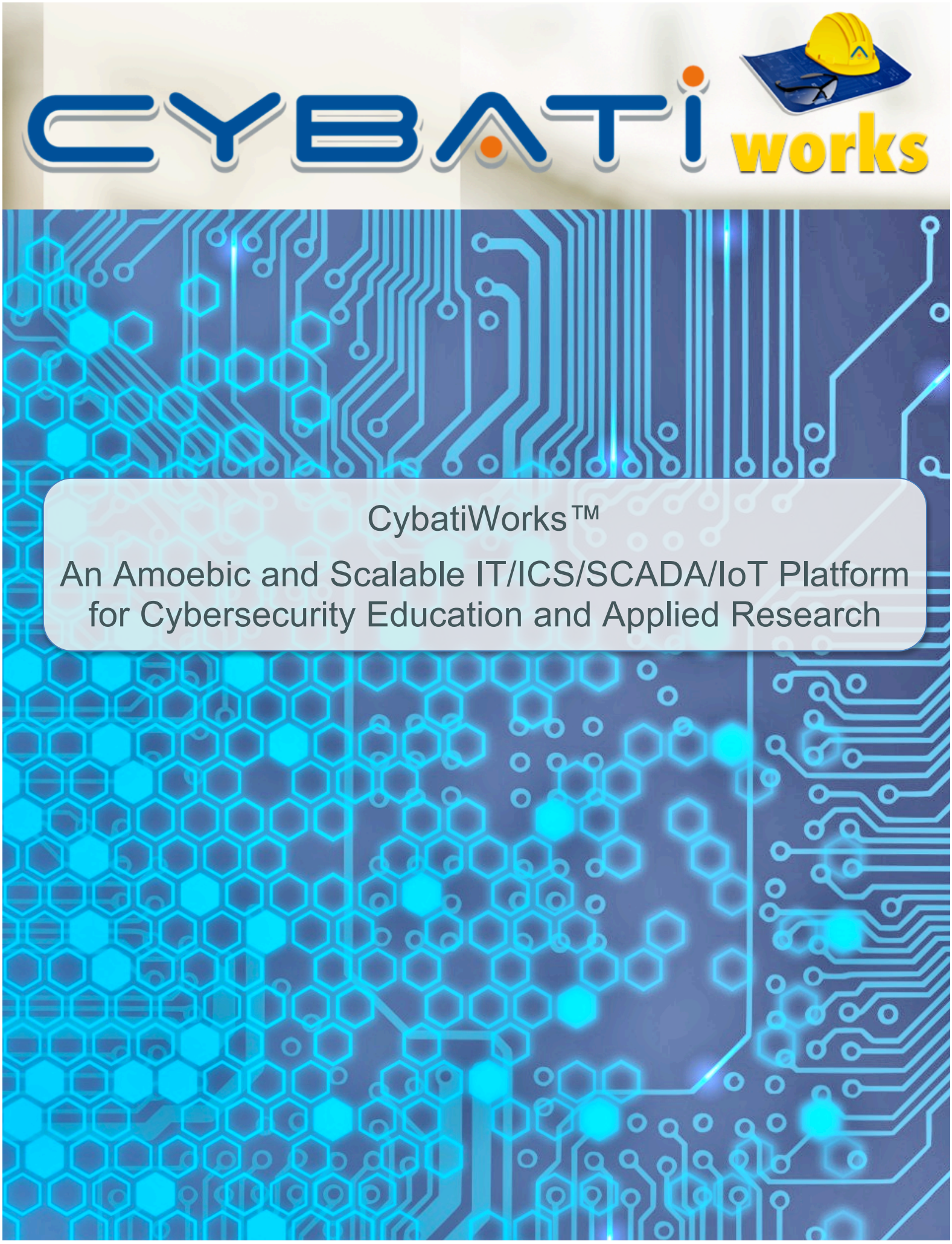
CYBATI
works
CybatiWorks™
An Amoebic and Scalable IT/ICS/SCADA/IoT Platform
for Cybersecurity Education and Applied Research

CybatiWorks™
An Amoebic and Scalable IT/ICS/SCADA/IoT Platform for Cybersecurity Education and Applied Research

Matthew E. Luallen
CYBATI Co-Founder

Abstract

ICS/SCADA cyber infrastructure is widely known to be a difficult and cost-prohibitive environment in which to establish a test bed and to further model threats and mitigating controls. A few thought leaders and institutions have developed successful models serving as excellent resources to the community; however, these models have proven difficult to share throughout the community due to cost, size and general technical difficulties. Furthermore the growing adoption of cloud computing and of the Internet of Things (Internet of Things) has provided an expansive set of tools to support the ICS/SCADA landscape. This paper discusses the CybatiWorks™ educational platform. CybatiWorks™ is a revolutionary, practical, scalable and currently available low-cost IT/ICS/SCADA/IoT platform for cybersecurity education and research leveraging four distinct elements: (i) environment simulation, (ii) IT/ICS/SCADA/IoT software, (iii) cyber security tools, and (iv) small-scale kinetic models. This foundational collaborative platform serves as a basis for standardized education and applied research for the IT/ICS/SCADA/IoT cybersecurity community.

1. Introduction

The increasing challenge of successfully protecting our national critical infrastructure was emphasized in the United States by President Barack Obama in early 2013 through Executive Order (EO) 13636[1] and Presidential Policy Directive (PPD) 21[2]. These messages clearly dictate the need for an informed and educated workforce to provide new solutions through enhanced education, products and services.

The critical nature and need of our modern electronically enhanced lifestyles serves as the foundational requirement to develop a massively scalable learning environment to understand the physical, operational and cyber security challenges within cyber-physical control environments. The solution discussed in this paper has evolved during a five-year developmental period to serve as an easily portable cyber-physical platform for cybersecurity education, product incubation and applied research.

2. Survey of Control System Security Laboratory Environments

Several governmental and academic institutions have developed control system laboratories to aid in the identification of cybersecurity risks, protect control validation and as models to educate personnel on how to better protect their systems. The need to have a well-defined test bed for the appropriate knowledge transfer is partially met through collaborative research environments available at a few entities. The following entities (not all inclusive) have built or are in the process of building extensive laboratory environments open for active industry participation for cyber-physical cybersecurity risk analysis:

- Mississippi State University
- Idaho National Laboratory
- Georgia Tech
- University of Texas at San Antonio
- Pacific Northwest National Laboratory
- TCIPG Participating Universities
- University of Houston
- Sandia National Laboratory
- University of Alabama

These environments serve as excellent examples of the demand for hands-on laboratory settings.

An alternate approach is to maintain the laboratory environments on the Internet allowing access to distributed resources[3]. This architecture provides a solution for traditional IT resources and serves as another excellent mechanism for scaling. The nature of cyber-physical systems is to sense and control their surroundings naturally supporting the desire for personalized, hands-on environments as one is

introduced to new concepts. Stationary centers of excellence provide unparalleled opportunities to focus on specific research goals; whereas highly portable and amoebic environments provide a wider range of solutions for a greater workforce.

3. Requirements of a Portable Control System Platform

Protecting and defending cyber-physical control system security requires an innate understanding of the processes being automated, the engineering design and tolerances, the supporting cyber assets and the workforce's operational procedures. Production cyber-physical control systems are large and costly thereby increasing the difficulty for a duplicate environment to be used for testing and educational purposes. Both professionals and academic students can gain considerable knowledge through a hands-on, portable living laboratory environment that leverage tools that are scalable from the classroom to the enterprise. Specifically the platform needs to be able to support international resources, as well as educational and applied research requirements including:

- Vulnerability assessment and penetration testing
- Attack surface and exploit code analysis
- Logic analysis and physical I/O control
- Industrial, building and home automation communications protocol analysis
- Engineering workstation and server operating systems
- HMI/MMI screens, points, tags and design
- Historian and OLE for Process Control
- Cryptography and steganography
- Kinetic model analysis
- Application security (e.g. web, database)
- Intrusion detection and analysis
- Physical I/O and supply chain analysis
- Electrically and mechanically safe to handle
- International voltages
- Instructor classroom and development tools
- Breakaway individual and group training
- Small and scalable physical footprint

The CybatiWorks™ Mini Kit and Industrial Edition platforms provide each participant with several of the hands-on capabilities of the $1.5 million CYBATI cybersecurity research facility. The platforms turn their office, home and hotel room into an easy-to-use, living laboratory.

3.1. Educational and Applied Research

The educational environment has been enhanced during the past four years while introduced to over 300 students at DePaul University's CNS 366/466 Critical Infrastructure [4], to over 2000 professionals using CYBATI's Critical Infrastructure and Control System Cybersecurity weeklong course, 15 private high school in Chicago, over 200 participants within the SANS Institute ICS 515 Active Defense 5-day course and further at several Universities such as George Mason and Villanova university.

3.2. Platform Hardware Components

CybatiWorks™ integrates common components combined with a customized quick connect I/O printed circuit board. The components include the appropriate elements for the platform to be completely built with an operational ICS controlled traffic light in less than 10 minutes and reset to factory default settings in 8 minutes. The CybatiWorks™ Mini Kit comes with everything necessary to operate in a VMWare® virtual machine. Electrical demands are limited to USB-only connected devices also powered by the participant's workstation. Each element was intentionally selected for the environment to scale and for platform support. For instance, an external Ethernet adapter is required to support VLAN tagging due to the lack of support within VMware's workstation vswitch. Table 1 details the specific hardware components included in the platform.

TABLE I. PLATFORM HARDWARE COMPONENTS

Platform Hardware Components	
Element	***Educational Outcome***
Storage Device with Software	USB flash drive or similar with instructions, restorable Raspberry PI image and a VMWare® or similar OS image based on a modified version of Kali Linux™
Raspberry PI 2, Case, SD Card and USB Reader/Writer	Serves as the logical I/O device, the device's storage and the ability reset the device to defaults
Customized Printed Circuit Board	Quick ribbon-connect circuit board with standard and extensible physical I/O with a standard Traffic Light intersection expandable to Elenco® Snap-Circuits, Fischertechnik®. The CybatiWorks™ I/O Board is easy to setup and is expandable for alternate design scenarios such as Power Grid, Oil and Gas, and Building Automation.
Sensors and Actuators	Up to 5VDC digital and analog sensor and actuators to represent unique kinetic models (e.g. motion, sound, light, liquid, motor control)
Cabling	Ethernet cable, USB power cable with push on/off button, USB Ethernet with integrated two-port USB hub

The CybatiWorks™ platform has been successfully usability tested on dual-core I3 Intel processors with a total of 4GB of RAM and utilizing virtualized environments with single-core processors and only 2GB of RAM. The platform includes several hardware and software elements that fit comfortably inside of a 9"x5"x3" case and pass all current Transportation Security Administration (TSA) and typical inspections.

3.3. Platform Software Components

The platform incorporates two storage devices, one for the participant containing instructional materials as well as the virtual machine and the other a SD card for the Raspberry PI. The virtual machine is configured for a 5-year old revision of VMWare, a 32-bit operating system based upon Kali Linux™ and limited host resources. The Raspberry PI operating system is built on top of the Raspbian Wheezy distribution that supports several of the same applications as the Debian-based Kali Linux™. All source code added to either software platform is included in the /opt/CybatiWorks/source directory. The selected software is either completely open source with a confluence of licenses that allow for redistribution and repurposing of the software or closed source trial editions that allow for redistribution and limited runtimes such as 2 hours. Individual participants may also explore extending the platform to include software that is not redistributable pursuant to license agreements, such as developer tools supporting smartphone emulation and engineering tools providing virtualized test harnesses.

The software incorporated in the platform has been selected to incorporate the skillsets of physical, cyber and operational personnel whom will use it for educational and/or applied research. Most software includes extensive online documentation to support the variety of uses; however, the CybatiWorks™ support community and education is also available inventory example configurations and use cases.

4. Five Distinct Elements to Support the Requirements

The educational platform incorporates five distinct elements to support the requirements outlined earlier in this paper. The requirements include cyber environment simulation, unique IT/ICS/SCADA/IoT software, unique cybersecurity software, and kinetic models. These five primary elements serve as the foundation for a simulated environment for cybersecurity education and applied research.

4.1. Cyber Environment Simulation

The cyber environment must be massively simulated to develop an educational and laboratory setting on a single workstation. Cloud computing, US Department of Defense (DoD) modeling initiatives and the IoT movement has provided amazing achievements in the past few years allowing for this flexibility. Specifically the need to openly incorporate software defined networking, traffic flow generators, and application containers serve as the basis for the architecture capabilities. A variety of each type of simulator was tested in a laboratory environment as well as in the field (e.g. curriculum and asset owner/operators) prior to the selection among each category. The table below highlights the three categories of simulators and their capabilities.

TABLE II. HOST AND NETWORK ENVIRONMENT SIMULATORS

Host and Network Environment Simulators	
Element	***Description***
Software Defined Networking	The host VMWare® machine and Raspberry PI image are pre-built with software defined networks to allow for shape-shifting, amoebic network designs beyond the single physical network port. (e.g. Naval Research Laboratory CORE MiniNet)
Traffic Flow Generators	Traffic generators support the multitude of security conditions that can be either created or replayed in to the environment (e.g. MGen, IPerf, D-ITG, Ostinato)
Application Containers	Application containers allow application portability across OS platforms and simpler configuration within the NRL CORE SDN (e.g. Docker, Java, WINE)

4.2. ICS/SCADA/IoT/IT Software

A variety of software is included with the CybatiWorks™ platform. The software selection is based upon the platform requirements and preference to open source software. License restrictions also determined what specifically could be redistributed. The software was categorically selected for distinct purposes such as a HMI or OPC server and engineering workstations. Some elements included exercises already developed by the community such as water gate PID loop design and fundamental routing protocol exercises using the NRL CORE software from the Brazilian RNP. More information about a selection of software included in the platform is available in the following table.

TABLE III. ICS/SCADA/IoT/IT SOFTWARE

ICS/SCADA/IoT/IT Software	
Element	***Description***
HMI. OPC, Historian	Specific applications to support ICS/SCADA modeling. (e.g. PeakHMI, PlantStreamer (OPC, Historian), PHPModbus HTML5, Inductive Automation Ignition (HMI, OPC, Historian), PVBrowser)
Engineering Workstation and Logic Controller	Development applications to support ICS/SCADA/IoT modeling (e.g REX Controls, MBLogic, RLL, Scratch)
Breadboard, Logic and Circuitry Simulators	Physical and logical circuit design to support basic to complex logic (e.g. PID Loops, QUCs, PeakHMI, MBLogic, Fritzing, Classic Ladder)
Networking	Network modeling, active routing protocols, multicast support, and protocol packet crafting (e.g. Scapy, NRL CORE, mininet)
Programming	Software development lifecycle, source code handling and analysis, and supporting libraries for integrated software (e.g. Qt, C++, Python, Ruby, Arduino)
Protocol Libraries	Specific IT/IoT protocol libraries for analysis and use (e.g. Modbus, S7, Ethernet/IP, AB PCCC, DNP3, IEC 61850, BacNET, Zigbee, WeMo, UPnP)
Device Simulator	Intelligent industrial device logic and protocol simulators (e.g. SNAP7, MBLogic, qModbus, pyModbus, PiFaceRTU)
IT Services and Applications	Full IT services and application capabilities configurable locally and within NRL CORE (e.g. DNS, DHCP, Radius, IPSEC VPN, Firewall, HTTP/s, Proxy, VoIP, Print, FTP, SMTP, Routing, Wireless, SMB)
Participant Exercises	Capture the Flag, Professional Missions, Secret Agent Technology Training Camp for Kids
Group Training	Integrated instructional support for group training using NRL Core, iTalc and networked missions
Instructional Support	A/V recording, assignment development, external physical camera, classroom desktop management and sharing (e.g. VLC, Freemind/HTML5 editor, articulating arm with camera)

4.3. Cybersecurity Software

The CybatiWorks™ educational platform leverages the Kali™ Linux operating system that includes an extensive set of IT cybersecurity penetration testing software. IT/ICS/SCADA/IoT cybersecurity analysis and testing tools have been layered on top of the image. Further additional toolsets to support cybersecurity education fundamentals, passive and active discovery, situational awareness and protocol analysis have been included. Security Onion, due to its popularity, is also provided to aid the participants in analyzing specific situations. Specific information about each category of software and elements included are in the following table.

TABLE IV. CYBERSECURITY SOFTWARE

Cybersecurity Software	
Element	***Description***
Fundamentals	Cryptography and Steganography, Password Cracking and Protection, System Auditing, Networking, Programming, Concept Flash Cards
Open Source Intelligence	Integrated search engine accessible ICS cybersecurity documents
Penetration Testing	Platform is based on Kali Linux™ with additional tools such as IRPAS, YERSINIA, Kautilya, and LOKI
Vulnerability Assessment	Supports the exploration of the automated and manual vulnerability assessment process (e.g. OpenVAS, binWalk, and Communication analysis)
Malware Analysis	Software investigation tools (e.g. Ollydbg, YARA, strings, hexedit, pdfextract)
Memory and Protocol Analysis	Packet capture, memory dump analysis utilities (e.g. YARA, Volatility, SNORT with QuickDraw rules)
Discovery	Integrated NSE Digital Bond Redpoint scripts supporting commands used by commercial engineering workstation tool active discovery as well as other tools (e.g. NMAP Redpoint, plcscan)
Awareness	Asset visualization and mapping software to identify host and communications modifications from baseline (e.g. CyberLens™, SNORT, syslog)
Controls	Firewall, IDS, Access, VPN, File System Monitor, anti-virus (e.g. fwbuilder with NRL CORE, SNORT, AAA, openvpn, afick, clamAV)
Security Onion	A pre-built ISO image for network monitoring, intrusion detection and log management (e.g. SNORT, Sguit, Network Miner, Suricata, Bro, Xplico)

4.4. Kinetic Models

In addition cyber-physical systems integrate the cyber world with the physical world through the dynamic logical automation of sensors and actuators. Each industrial system represents a distinct set of elements and supporting logic to analyze. Further, the security solution may be a physical adjustment, operational change or cybersecurity control that mitigates the most risk at the least cost. Kinetic models allow the participant to explore specific design constraints. A very common model is a traffic light intersection with an easily understood attack vector of all lights on, all lights off or all green. Figure 1 depicts the CybatiWorks™ Mini Kit with a sample traffic light intersection kinetic model connected to the Raspberry PI and necessary cabling.

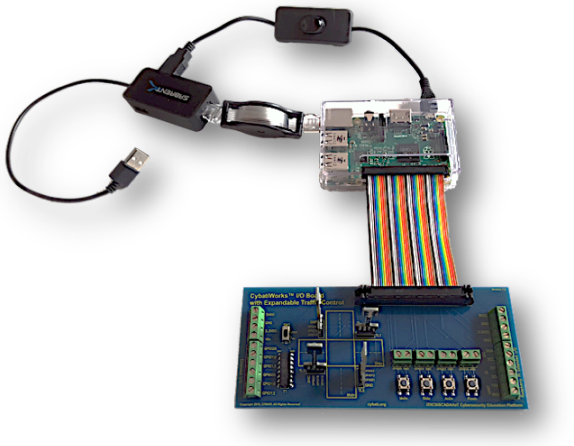

Figure 1. CybatiWorks™ Mini Kit

The models are represented on printed circuit boards allowing the platform to also support circuitry validation and bus snooping through exposed UART, SPI and I2C circuits. Each model is also designed for quick-connect support for commercial logic devices from Siemens, Rockwell, General Electric, Schweitzer Engineering Laboratories and others. The table below explores the capabilities of the PCB kinetic models provided for the platform.

TABLE V. KINETIC MODEL SUPPORT

Kinetic Model Support	
Element	***Description***
Physical Analysis	Traffic Light, Building Automation (Heating, Venting and Air Conditioning / Fire Supression), Oil and Gas, Assembly Line, Power Grid, Crane
Logic Validation	Integrated correct and rogue logic and HMI/OPC for European and American Traffic Light patterns to support logic analysis and supply chain validation (e.g. RexDraw, Ignition, PeakHMI)
Circuitry Validation	2-layer printed circuit boards to support supply chain validation
Bus Snooping	Exposed I2C, SPI connections and breadboard extensions
Commercial Devices	The Mini Kit ribbon cable I/O is expandable via CybatiWorks™ adapters and external network switches to support the Industrial Edition kit commercial devices (e.g. Siemens, Rockwell, Opto22, Schneider Electric, Phoenix Contact, Schweitzer Engineering Laboratories)

4.5. Expandable

The educational platform supports expansions based upon the participants needs. The I/O board supports alternate kinetic models such as assembly lines, smart grid and wireless cranes using the integrated screw terminals. Network models can be expanded using the integrated capabilities of the Naval Research Laboratory's CORE software combined with the easy-to-use CybatiWorks™ wizards. The network models can support an integration of virtualized system and systems that cannot be virtualized using an expansion network switch such as the Cisco Systems® SG-200-08 small business switch. The Mini Kit is also expandable in to the CybatiWorks™ Industrial Edition elements using real ICS devices from popular vendors such as Siemens, Rockwell, General Electric, Schneider Electric, Opto22, Schweitzer Engineering Laboratories, and Phoenix Contact as shown in Figure 2.

Figure 2. CybatiWorks™ Industrial Edition

5. Platform Capabilities

The CybatiWorks™ educational and applied research platform has been vetted by thousands of participants. The original construction required multiple uniquely configured virtual machines and days of laboratory construction to model simple cybersecurity attacks and mitigating controls such as Ettercap MitM. The CYBATI cybersecurity research facility is composed of over 100 physical nodes, each individually maintained using a very time-consuming and arduous process. The CybatiWorks™ amoebic and scalable platform provides a single individual with amazing power to create up to a 300 nodes uniquely configured and with an operational network at one moment and a completely different design of applications, nodes and subnets only minutes later. This amoebic design includes specific mechanisms for rapid prototyping, traffic generation, active defense and quickly accessible simulation wizards. The participant is provided with the capabilities of a $1.5 million ICS cybersecurity research laboratory that is highly portable.

5.1. Rapid Prototyping / Amoebic Networking

The CybatiWorks™ platform supports several rapid prototyping capabilities. Specifically tested

capabilities include a) product data rate, protocol and network awareness, b) security control validation, c) capture the flag events, d) amoebic networks, and e) honey networks. The integrated software layered inside of the Naval Research CORE network simulator supports rapid prototyping. The platform is further validated by the SCADAVT design discussed by Dr. Amalawi in his paper "Designing Unsupervised Intrusion Detection for SCADA Systems"[5]. NRL CORE was derived from the open source IMUNES project, can be scaled across multiple COREs, can be connected to multiple live networks and is extensible and easy to use.

CYBATI tests have validated support for 16,000 unique and communicating nodes across 4 core instances. Each unique node can be independently configured to use the host VM applications as well as dynamically adjusted during runtime, hence the phrase amoebic networking. The platform easily supports multiple physical node systems incorporated in to the NRL CORE platform. NRL CORE supports VLAN tagged interfaces allowing the platform to be directly coupled to a switch supporting VLAN trunking. Figure 3 depicts NRL CORE configured with 8 VLANs (0, 200, 300, 400, 500, 600, 700, 800) using a Cisco Systems 200 series micro switch. The scalability of the platform extends from the dual-node Mini Kit participant to over 300 simultaneous nodes on the same workstation.

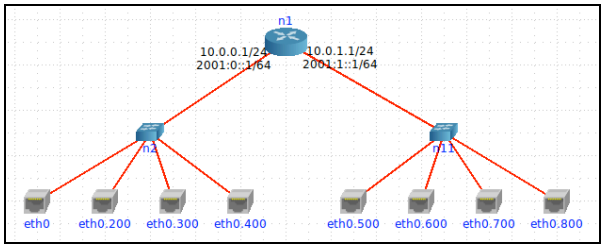

Figure 3. NRL CORE Physical Connections

5.2. Traffic Generation

Specific situations require pre-captured or unique data flows. The platform is pre-equipped with four popular, proven and scalable traffic generators – iPerf, MGen, Ostinato and D-ITG. The four traffic generators support the variety of unique instances typically occurring within testing scenarios: 1) statistic distribution of traffic such as poisson and variable amounts of jitter and baud rate, 2) intelligent traffic flows for IT and industrial protocols such as VoIP, HTTP, DNS, routing, Modbus/TCP, S7, DNP3, IEC 61850, and BACNet 3) denial of service traffic conditions. NRL CORE coupled with the traffic generators support the automated and/or dynamic enabling of traffic flows for specific situational tuning.

The CybatiWorks™ platform also incorporates a traffic generation wizard using open source ICS protocol libraries for Modbus, DNP3, S7, IEC 61850, and BACnet. The protocol generator wizard creates live protocol datastreams of actuator/sensor/meter data. These real data streams can be used to test attack scenarios and validate security designs and controls.

5.3. Simulation Wizards

Simulation wizards provide predefined, reproducible environments for the participant or researcher to review. The wizards focus the participant on the specific educational outcomes without the common challenges of command line typos, mis-ordering of application dependencies or lack of sufficient resources.

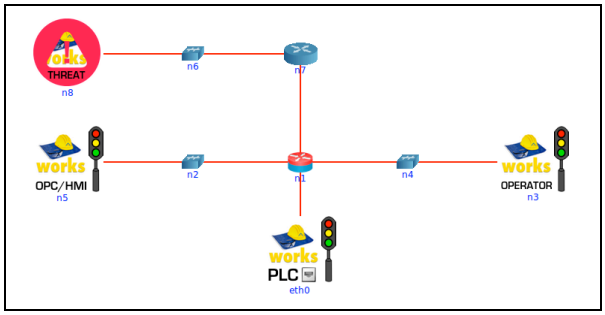

Figure 4. Simulation Wizards

The first wizard developed was to emphasize the lack of authentication within industrial protocols such as Modbus/TCP leveraging an example network design as shown in Figure 4. The wizard uses the NRL CORE software to virtualize a multi-node network. The participant is then stepped through the following process: a) introduce an Ettercap MitM exploit to blind the HMI operator, b) educate the participant about the type of exploit and mitigating control c) introduce ARPwatch to prevent and alert upon the specific type of attack. The simulated attack was proven to work in a physical laboratory environment prior to its virtualization in the participant's setting. The entire process – building, breaking and securing can be completed in as quickly as 60 seconds and then is ready to be performed immediately again. Typically a participant should take at least 120 minutes to operate the wizards and review the associated learning material. CybatiWorks™ educational material is coupled with the educational platform to emphasize what the wizard has performed. The wizards compel the participant to understand what has happened while the CybatiWorks™ educational material reverse engineers the wizard's steps. Additional wizards are discussed in the following table.

TABLE VI. SIMULATION WIZARDS

Simulation Wizards	
Wizards	***Capability***
Industrial Protocol MitM	Builds a virtualized multi-node network while stepping the participant through an Ettercap MitM exploit
Web/Application OWASP Tutorial	Builds a vulnerable Web Application training environment based upon the OWASP 2011 and 2013 top vulnerabilities.
Industrial Protocol Firewall	Builds a virtualized multi-node network communicating an Industrial protocol across a multi-network firewall. The participant builds firewall rules to support valid communication.
Honey IT/ICS Network	Builds a multi-node network with high interaction threat intelligence honeypot tools such as MBLogic, Conpot and Dionaea
Simulated ICS	Builds a quick ICS environment across the Loopback interface using a multi-node network and MBLogic for soft ladder logic and HMI display
VirtuaPlant	Simulated bottling plant depicting specific attack and mitigation options
Mini Kit Traffic Light ICS	Script to quickly load the Traffic Light function block code to the Raspberry PI and launch the operational HMI using the CybatiWorks™ I/O Board

6. Pedagogy, Industry Outreach and Future Enhancements

Initiatives such as the NIST 800-82 cybersecurity guide and the NICE Framework provide direction on specific cybersecurity elements as well as educational outcomes to include within a curriculum. Furthermore a recent paper presented at the ASEE conference developed a set of lessons for K-12 participants [6]. The educational and applied research platform next steps are to associate specific learning objectives with simulated scenarios and industry standards. Future enhancements will be based upon the outcome of industry guidance through the CybatiWorks™ user community.

6.1 Educational Scenarios

Specific educational scenarios have been developed within the platform to support specific learned outcomes. These scenarios are called missions and provide the participant with a specific achievement. The gain the achievement and unlock access to the next mission the participant must perform a series of steps to understand and then either attack or mitigate a specific cyber element. The missions are categorized as offensive, defensive, construction and kids as shown in the following table.

TABLE VII. MISSION CATEGORIES

Mission Categories	
Category	***Description***
Blue	Defensive cyber, physical and operational capabilities
Red	Offensive cyber, physical and operational capabilities
Construction	Design and build missions and platforms
Kids	Explore electronics, code and technology

The platform supports knowledge outcomes aligned specifically with the NERC CIP reliability standards, IEC 62443 and NIST 800-82 guidance.

6.2 Future Enhancements

With the last iteration of enhancements, the platform has shrunk in physical size, number of components and costs while increasing in capabilities and intrinsic value. Future enhancements will be to specifically tailor the education to validated knowledge outcomes. Elements that are under development include but are not limited to:

- Dynamic blackbox network, host and application generation for participant discovery
- Automated threat generation for participant threat classification (e.g. Nation State, Hacktivist, Criminal, Insider) and analysis
- Pre-assessment evaluation for identifying only necessary education scenarios
- Kinetic model development (Oil and Gas)
- Post-assessment evaluation for skills validation

7. Conclusion

Cyber-physical system security requires a hands-on approach to understanding and protecting the system. The CybatiWorks™ amoebic and scalable portable control system platform greatly simplifies the process to understand the technology, the process being automated and the engineering behind individual and coupled physical components. The expandable platform supports breakaway individual training with the ability to couple together for group training and collective tasks. The CybatiWorks™ Mini Kit can be expanded to support the commercial devices included in the Industrial Edition to further apply the skillsets using real world devices. CybatiWorks™ removes the painstaking process of laboratory setup and dependencies allowing the students, educators and researchers to focus on their specific cybersecurity goals. Contact CYBATI today for a demonstration and more information about our education and research.

8. References

[1] White House. Executive Order 13636: Improving Critical Infrastructure Cybersecurity. https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/eo-13636. Feb 2013

[2] White House. Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil Feb 2013

[3] Christian Williams, Thomas Klingbeil, Lukas Radvilavicius, Antanas Cenys, Christoph Meinel. A Distributed Virtual Laboratory Architecture for Cybersecurity Training. Hasso Plattner Institute. Dec 2011

[4] Matthew Luallen, J.P. Labruyere. Developing a Critical Infrastructure and Control Systems Cybersecurity Curriculum. HICSS-46, January 2013.

[5] Abdul Mohsen Afaf Almalawi, Designing Unsupervised Intrusion Detection for SCADA Systems, RMIT University. Dec 2014

[6] Brandon Gregory Morton, Youngmoo Kim, Matthew Nester VanKouwenberg, Chris Lehmann, Jessica Ward. Developing Curriculum for Introducing Cybersecurity to K-12 Students. June 2014