Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)
Issues (49) 2021
ISSN: 2616-9185
www.mecsj.com

Shared Testing Environments to Address the Shortage in IIoT and New Industry 4.0 Technology Testbeds

Eng. MISHAL AL-AHMARY
maa07407@marymount.edu
Cybersecurity Doctoral Student, Marymount University

Abstract

Industrial internet of things (IIoT) is the cornerstone for communications in Industry 4.0. The complex technology used in new Industrial Control Systems (ICS) networks requires advanced and well-equipped testing environments. However, finding an open testbed for IIoT research is challenging. This paper will elucidate the issue of shortages in testbed and development environments in Industry 4.0 and IIoT in particular. Three IIoT open testbeds (FIT IOT-LAP, Tutornet, and iTrust) that researchers and students can use for training and research will be explored in this paper. The accessibility and the type of equipment available are the main aspects used herein to analyze each testbed. The main factors and challenges of building open testbeds for IIoT and the latest ICS technology are studied. Furthermore, the advantages and disadvantages of these three testbeds will be explained so researchers and students can make use of these available labs in research. The paper will conclude with recommendations that can

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)
Issues (49) 2021
ISSN: 2616-9185
www.mecsj.com

bridge the gap in testbed availability and how that can enhance research and workforce development.

Keywords: IIoT, ICS, Cybersecurity Testbeds, Industry 4.0, MQTT.

1. Introduction

Continued education and training are cornerstones for organizations to maintain sustainable growth and their competitive edge in relation to rivals in the same industry. Government agencies and public institutions are also taking a greater interest in workers' education and training to further develop their capability and productivity. Recently, many government agencies have started focusing on attracting the talented workers and professionals instead of outsourcing the entire job to contractors. To achieve these goals, their hiring strategies require upgrades, as the current development plans and procedures are outdated and cannot meet the organizations' objectives. For several years, courses in common management and personal skills were taught through typical modes of education, such as theoretical classes and lectures led by instructors and trainers. Only in the last decade or so have new technologies been used to digitalize content so users can attend courses remotely through their personal computers. For example, many organizations now periodically release online sessions for workers and trainees who need further development in common skills and knowledge fields. These courses cover basic management skills and the new policies that workers may need to know in order to perform their daily tasks. These types of sessions and training materials mainly comprise text and some theoretical content that is easy to design and publish with minimal cost and effort. An online server with an access management system is all that an organization needs

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)
Issues (49) 2021
ISSN: 2616-9185
www.mecsj.com

to release such online materials, and, in turn, an unlimited number of workers and trainees can benefit from the training.

1.1. The Complexity of New Information Technology Systems

The rapid growth in information technology (IT) has introduced an enormous number of new systems and tools. These new systems and tools are widely used among all organizations and institutions, including governmental, banking, educational, and health care organizations as well as all other critical infrastructures. The nature of these technologies and the complexity of their systems make it imperative for individuals who operate and control them to have deep knowledge and skills. In other words, these new technical fields are completely different than the nontechnical fields in terms of training and workforce development process. The constant change in IT and different applications of these IT systems in our lives have rendered the typical training and workforce development approaches outdated and inadequate to meet the needs of workers and employers to maintain a high level of knowledge and skills for the smooth operation of these complex systems. Therefore, there is an urgent need for new robust training systems and interactive development programs that take into consideration the nature of jobs, workers' responsibilities, and daily work activities. Practical training and hands-on materials are the priority among the mandatory requirements for IT workers' development. Relying only on the theoretical content for these advanced technical fields, such as networking, software, and servers' management, is inadequate and cannot be beneficial for workers unless tied with practical content through testing labs that simulate real systems.

2. Cybersecurity Education Challenges and Testbed Shortage

Cybersecurity is one of the most complicated fields of IT and needs very sophisticated learning environments and materials. The wide number of technologies and systems used in ICS makes it hard for workers and professionals to gain comprehensive knowledge about the entire

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)
Issues (49) 2021
ISSN: 2616-9185
www.mecsj.com

stack of technology without a continuous training programs and testing environments. In professional labs or testing environments, the conventional learning approach is not effective for ICS cybersecurity workforce development. There is a critical need for labs in cybersecurity training programs more than most other fields in IT. However, developing and implementing a real training lab for cybersecurity is very costly, and it may end up creating an entire development environment similar to the production environment, which is logically unacceptable from a business perspective. Moreover, the overlap between systems and solutions in ICS is a serious challenge for cybersecurity professionals. In other words, controlling the cybersecurity for the entire ICS and automation stack can be difficult if left to cybersecurity professionals only, without support from ICS and Supervisory Control and Data Acquisition (SCADA) engineers (McBride et al., 2020). Using labs or testbeds is the only way to investigate the compatibility of new security controls and policies before they are deployed for production systems. However, as cybersecurity operations rely on high-level testing and investigations, trainers and students may face serious challenges when trying to test cybersecurity solutions and practicing what they have learned in class. Therefore, it is important to determine the possible solutions that can help in achieving these objectives without imposing any threats to the production environment or having students and trainees incur large costs.

3. Systems Integration and the Convergence of IT & OT

ICS play a vital role in manufacturing and critical infrastructure operations. Over the last two decades, IT systems have evolved, helping many industries to expand their operations and production. Utilizing new technologies and advanced IT system components in any industry or business helps organizations gain a competitive advantage over their rivals. The revolution in IT is also reflected in operational technology (OT), as many systems that were originally developed for the IT environment have been extended to the OT networks. Most corporations in the

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)
Issues (49) 2021
ISSN: 2616-9185
www.mecsj.com

industrial sector have started an integration process between systems from both IT and OT environments to optimize their operations. In general, the ICS structure has changed due to these breakthroughs in IT. The current cybersecurity frameworks in information and operational technology were designed to be compatible with the typical systems' structure. ICS cybersecurity frameworks also face the same issue where most of the current frameworks were originally developed to work with conventional OT devices and systems. OT networks have a wholly different environment than typical IT networks; all ICSs are mainly built for a specific purpose, which means that all communication and systems behaviors are predictable and known. Therefore, any fluctuation in normal network behaviors or patterns is reported as a threat, which is one of the main obstacles for cybersecurity detection and reconnaissance tools (Kim et al., 2016). Furthermore, ICS has many industrial control protocols, and each of them has a different design and packet structure; deep industry knowledge is required to deal with all these industrial protocols before implementing any security solution (Drias et al., 2015). This explains why most of these protocols are very sensitive to regular security operations, such as scanning tools and packet investigations. Moreover, security tools and controls are usually deployed in most systems' components, including network traffic, authentications, software, and hardware compliance. For example, to secure a network, it is important to apply packet investigation tools or intrusion detection systems so all suspicious traffic can be eliminated (Feng et al., 2017). The way these tools work can demonstrate how deeply security controls are involved in all parts of the ICS network. Therefore, proof-of-concept testing is essential in ICS and OT networks before deploying any new security solution to ensure that these tools are not in conflict with any other components in the systems (Green et al., 2020).

ICSs and OT networks have complicated backup and restore processes compared to IT systems. It is much easier to retrieve and backup data when something goes wrong in the IT environment, which makes IT professionals more confident in deploying timely updates and patches for the production systems. However, the scenario is totally different for ICSs, as

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)
Issues (49) 2021
ISSN: 2616-9185
www.mecsj.com

availability and business continuity are first priority, even exceeding security for ICS in general (Shin, 2017). Therefore, in order to avoid this complexity, organizations and ICS professionals prefer a completely separate development environment or testbed to investigate all new security controls and tools before they are deployed to the production environment.

4. IIoT as the Core Technology for Industry 4.0 and New Automation Stack

In the last decade, there has been a dramatic change in business control and management approaches, as many manufacturers have employed new technology to optimize the production process. Historically, there were specific conditions and circumstances that caused each industrial revolution. IT and OT convergence has led to radical changes in manufacturing tools and ICS systems, which have reshaped most of the current manufacturing approaches and strategies. The enormous capabilities of these new technologies in the industrial sector was a quantum leap for OT systems, as many industries adopted these new technologies for their production lines. It is important for all industrial organizations to have a wider view of all business stages, from basic manufacturing lines to distribution and end customers. For all conventional manufacturing approaches, controlling all these stages of production and distribution without involving other systems from the IT network is challenging. For example, integrating the market analysis, supply chain process, and warehousing systems with the production lines will help optimize the entire production process and be reflected in sales and revenues. Thus, it is very useful to, for instance, have an instant overview of warehousing, so any shortages can be planned for in advance. Moreover, the supply chain units can optimize the storage and warehousing units if they can predict the exact number of products that will arrive at shipping and storage facilities.

Controlling and optimizing raw materials and all other manufacturing inputs are essential for the industrial cycle, as any interruption or fluctuation in the availability of these materials will impact the entire manufacturing process, including supply chain and warehousing

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)
Issues (49) 2021
ISSN: 2616-9185
www.mecsj.com

divisions. Therefore, controlling the manufacturing resources and all other levels of the production processes via the main manufacturing control systems will help achieve greater resource optimization and production efficiency. Typically, the Manufacturing Execution System (MES) is the main unit in ICS for controlling and managing resources and raw materials. Enterprise management systems (ERPs) also play a vital role in running core management functions, such as those related to finance and marketing. Moreover, precisely knowing the available resources and level of business resilience in terms of operations and sales is beneficial for the manufacturing process. Therefore, business analysis is a very important tool for organizations' management and leadership. These days, the right decision must be made after gathering adequate data and information from different levels in the manufacturing stack, so it is mandatory to connect the entire manufacturing process and stages together to analyze the generated data. This also helps identify the weakest parts within the entire manufacturing system so that these weaknesses can be ameliorated. For example, any limitation in warehousing or supply chain capabilities can impact the complete manufacturing process.

4.1. The new Industry 4.0 model and IIoT

Industry 4.0 was introduced in the last decade to meet the increased need for smart cyber-physical systems. In other words, the Industry 4.0 model is a practical implementation of new manufacturing systems that involve advanced technologies from both IT and OT environments (Murray et al., 2017). There are different approaches to implementing the Industry 4.0 model; each approach focuses on specific capabilities required in the overall manufacturing process. What matters to us here is the new automation stack structure suggested by the Industry 4.0 model, which organizes the integration between all the different layers in new ICS and OT networks. Through the Industry 4.0 automation stack, all the different levels and systems within the manufacturing systems can share and exchange information, which is very useful in improving productivity and lowering costs. According to Purdue

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)
Issues (49) 2021
ISSN: 2616-9185
www.mecsj.com

Enterprise Reference Architecture (PERA), one of the most prominent Industry 4.0 automation models, there are five main automation layers; each of these layers has a unique function. These layers are physical processes, intelligent devices, control systems, manufacturing operations systems, and business logistics systems. Some new forms of this model added a layer called the enterprise network (Ackerman, 2017). The new automation stack relies on the Industrial Internet of Things (IIoT) as the main medium for communication and information sharing. The flexibility and usability that IIoT can provide to ICS has led most equipment manufacturers to update their devices and systems to be compatible with this promising new technology. Cables and wired communication mediums can sometimes be very confusing for technicians and engineers, especially in large ICS units. Moreover, adding a new device requires only a few clicks in IIoT instead of installing a new cable across the ICS. There are other factors that have made IIoT the backbone of communications in the new automation structure, for example, the type of protocol used in IIoT communication.

4.2. MQTT and IIoT Communication Protocols

Message Queuing Telemetry Transport Technical (MQTT) is the main protocol used in IIoT. What makes MQTT more valuable in IIoT compared to conventional industrial protocols is its versatility; it can easily be used in different environments and systems. For example, MQTT has been used in both IT and OT networks and is compatible with most of IoT networks including personal IoT devices. The MQTT protocol has the unique feature “publish and subscribe” so each specific device can be configured to receive a particular group of packets (Hunkeler et al., 2008). It also helps optimize the network bandwidth by eliminating unwanted traffic. From a security perspective, MQTT has a very interesting feature—the isolation between all network devices—as all communication comes through the main brokers. In other words, each device can contact only the main broker. Moreover, MQTT has a very small packet size with a minimal overhead, which results in lightweight messages that can be sent rapidly (Bellavista et

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)
Issues (49) 2021
ISSN: 2616-9185
www.mecsj.com

al., 2016). MQTT is very useful in terms of scalability and upgradations. As all devices are connected to the broker, no extra configuration or updates are required for other devices in the network when one needs alteration. The most useful feature in MQTT is the “quality of service levels”, which makes this protocol highly reliable, as each packet can be traced and confirmed to have been delivered to the destination.

5. IIoT Open Testing Environment and Testbed Shortage

The new industrial and automation models have greater complexity and integration, which means more research and testing environments are needed to investigate all new and potential threats. Researchers, students, and trainees need modern testbeds and research environments that employ the latest protocols and techniques used in the new industry models. The cost required to install these advanced testbeds is the main obstacle for students and researchers who work on self-funded research. Therefore, in the following analysis, I will attempt to find free testbeds for IIoT that students and researchers can use to conduct their research and studies, without incurring any further cost. Different factors will be analyzed in all the suggested testing environments, such as the accessibility, hardware and software used, and the limitations of these testbeds. The main aspects of this analytical study that should be of interest to researchers and students are the cost and accessibility of these testbeds.

5.1. The Future Internet Testing Facility (FIT IOT-LAP)

The scale of the project important to determine the equipment and testing tools needed. New small computing units, such as Raspberry PI and Arduino, have enabled students and researchers to conduct small experiments and testing projects due to their affordable prices. However, in large-scale experiments that require many nodes, these solutions are not enough, as researchers need a large number of testing nodes, which is very costly. Therefore, the Future Internet Testing Facility or FIT IOT-LAB was introduced by the OneLab consortium,

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)
Issues (49) 2021
ISSN: 2616-9185
www.mecsj.com

which constitutes five main higher education and research institutions, including Sorbonne Université (SU), National Institute for Research in Digital Science and Technology (Inria), iMinds Technology Systems, and Technical University of Berlin. The FIT IoT-LAB is unique because of the monumental scale and the large number of nodes and sites used in this lab. FIT IoT-LAB contains more than 2700 nodes from different types of IoT hardware. It has three main models of IoT nodes from different generations and levels of hardware. The first model of nodes used in FIT IoT-LAB is WSN430: MSP430, which is appropriate for legacy systems and useful for specific types of sensors, such as temperature sensors. M3 is the second type of node in this lab; it is relatively modern. The latest and most capable node in FIT IoT-LAB is A8, which is a high-end IoT device used in many applications of IoT networks (Fambon et al., 2014). There are other hardware components used in this lab for connecting and controlling the IoT network, such as the gateway and control node.

The geographic locations and distance between sites are essential for some types of experiments and projects. Therefore, FIT IoT-LAB was developed in eight remote geographic sites to determine how distance and remote sites can change the outcomes of the testing and experimental projects. It also features a group of open-source software added by default to the lab platform so that a wide range of experiments and testing projects can be applied in this lab. Building good hardware equipment in the lab without the required software may limit the output and test results in the lab (Adjih et al., 2015). FIT IoT-LAB uses Linux OS on the A8 node model, which enables many external applications to use the API interfaces for collecting data and extending the results for more tools and systems. For example, in some projects, it is important to have a realistic representation of the node. API can help extend the outcomes to other tools to visualize the final result and current changes (Harter et al., 2015). In addition to Linux, users can utilize RIOT, OpenWSN, FreeRTOS, Contiki, and TinyOS software, which is available in the lab. Finally, accessibility is an important factor for users, especially in testing and research. Researchers may need to repeat their testing multiple times to find the most accurate

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)
Issues (49) 2021
ISSN: 2616-9185
www.mecsj.com

results they are seeking, so it is vital to have smooth and easy access to the testing platform. It is very easy to sign up to and start your testing instantly with FIT IoT-LBA if you have a business or educational institution email address. Also, the web interfaces used in the lab are very useful and easy to use, so the user does not need a tutorial on how to use the lab.

	Grenoble	Lille	Paris	Strasbourg	Rennes	Institut Telecom	**Total**
WSN430 (800MhZ)	256	-	-	256	-	-	512
WSN430 (2.4GhZ)	-	256	120	-	256	-	632
M3	384	320	24	120	-	90	938
A8	256	-	200	24	-	70	550
Host Node	32	64	–	–	–	–	96
Total	928	640	400	344	256	160	2728

Figure 1. Users can select and reserve the number and type of nodes they wish with (Fleury et al., 2015).

5.2. Tutornet: A Low Power Wireless IoT Testbed

The shortage in research equipment and laboratories for Industry 4.0's new technologies drove Viterbi School of Engineering at the University of Southern California (UCS) to build their own lab for research and testing to provide students with hands-on and more practical experience with these technologies. It was designed with greater focus on IoT technology and it is located at Ronald Tutor Hall in UCS. The lab consists of 113 sensor nodes chosen from three different generations, TelosB, MicaZ, and OpenMote, with a 2.4 GHz radio frequency band, which helps cover a wider range of research and tests (Viterbi, n.d.). The lab is situated on two floors, which gives more space for nodes to be distributed across a larger area.

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)
Issues (49) 2021
ISSN: 2616-9185
www.mecsj.com

THE THREE GENERATIONS OF MOTES DEPLOYED ON TUTORNET.

Mote	Manufacturer	Year	Microcontroller	Flash size	RAM size	Transceiver
MicaZ	CrossBow	2004	Atmel 8-bit ATmega128L @ 8 MHz	128 kB	4 kB	CC2420
TelosB	MoteIV	2005	TI 8-bit MSP430F1611 @ 8 MHz	48 kB	10 kB	CC2420
OpenMote	OpenMote	2015	TI 32-bit CC2538 @ 32 MHz	512 kB	32 kB	2.4 GHz SoC

Figure 2. Sensor nodes employed in the Tutornet (USC, n.d.)

The Tutornet lab architecture features three tiers. The first is the central server, which is responsible for leading the communication between different nodes and users. The central server uses Linux OS and hosts an Apache-based web application for managing and controlling the reservation system in addition to user privilege control software. The second tier is the concentrator that connects central servers to the nodes. The concentrator nodes use budget software and hardware such as raspberry-pi and Ubuntu Linux, which help control the budget and reduce costs significantly. To keep servers and nodes connected, the lab has 13 connectors that use USB ports (Viterbi, n.d.). The third tier in this lab is the end-point nodes, which utilize the USB port for both communication and power.

Although the Tutornet lab provides a good environment for IoT and wireless network sensors, it is limited only to this type of technology, and it is not clear how this lab will perform when additional components of ICS have to be integrated with IoT nodes. One of the prominent advantages of this lab is the space available for nodes, as each floor in the lab spans over 150 square meters, which is useful for testing the wireless nodes' range and connectivity. The lab also provides pre-generated datasets for free in case researchers need only the data. In this way, they can save a lot of time by using the available datasets. The accessibility of this lab has some restrictions, as students and researchers need to contact the lab management in advance rather than signing up online to use the lab. Also, the lab lacks API, so users, instead of redirecting outputs, will need to transfer the generated datasets to other systems physically.

5.3. iTrust - Internet of Things (IoT) Automatic Security Testbed

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)
Issues (49) 2021
ISSN: 2616-9185
www.mecsj.com

The iTrust testbed is a unique IoT testing environment that covers important aspects required by cybersecurity research to validate the security and usability of IoT devices. The lab was designed and built by Singapore University of Technology and Design (SUTD) for researchers and students to apply their IoT security research in a real environment. The research and results that come from the iTrust testbeds are more credible and trusted because they are supported by a recognized institution such as Singapore University. Moreover, what gives research in this testbed more credibility and trust is the other useful testbeds for ICS, water treatment plants, and electric power stations, which are provided by the same institution. Nowadays, IoT is an essential part of ICS and Industry 4.0 manufacturing models, so it is important to study the impact and exposure to threats in ICS networks and power stations in this technology; in other words, students can take their IoT research further by extending it to these available labs to study the conflict or impact on new ICS units (Hankin et al., 2018).

IoT devices can be affected by nearby objects and the surrounding environment; for example, walls and barriers usually undermine the connectivity of wireless devices. Furthermore, electromagnetic interference and external disruptions can impact wireless networks; therefore, the iTrust lab was designed and placed in a shielded room, which will enhance the accuracy of results and findings for the research performed in this lab (Siboni et al., 2019). The lab uses the latest IoT technology it is more focused on security-related research which means newer forms of threats and vulnerabilities can be investigated in this lab, as. The iTrust lab is equipped with sophisticated technologies from the top ICS manufacturers, such as Rockwell Automation, National Instruments, Schneider Electric, and Siemens. Some of this equipment was provided by the manufacturers as a contribution to build a modern testbed that can benefit several researchers and students. What makes this lab very useful is the full ICS stack available, including all types of ICS devices, such as remote terminal units (RTUs), human-machine interfaces (HMIs), and programmable logic controllers (PLCs).

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)
Issues (49) 2021
ISSN: 2616-9185
www.mecsj.com

Although the iTrust lab is very advanced and well equipped, it has some limitations, such as the lack of remote access for some testbeds, which is still under construction, and it is not clear when it will be ready for use. Access to the iTrust lab is free for iTrust members and Singapore University students. However, researchers who are not from Singapore University will need to apply for the Student Researchers Program (SRP) to access the iTrust lab. In comparison to the aforementioned labs, accessibility is the biggest challenge for researchers in the iTrust lab. Researchers have to apply for a research program to use the testbed, which requires time and communication with the testbed management team. However, there are paid memberships for corporations and organizations to access the lab.

6. Findings and Results

Strengthening the security of critical infrastructure requires more investment in research and workforce development. Both public and private organizations have a greater interest in building professional cybersecurity teams to handle the increasing number of cyberthreats. Workforce development and academic research for technical fields, such as cybersecurity, need advanced infrastructure and learning equipment. Labs and testbeds are the topmost necessity among the tools needed to enhance cybersecurity education and research, especially for ICS and Industry 4.0 technology. IIoT is one of the most important technologies in new ICS and OT systems, which require more researchers and training programs. However, it can be difficult to find open labs and testbeds that can help trainees and students gain hands-on experience or apply the theoretical content to real-life scenarios. Researchers may also face the same challenge when trying to validate their findings and research. The three open testbeds introduced in this paper can be utilized by students and researchers or by organizations to train their workforce on advanced cybersecurity solutions. I found FIT IoT-LAB to be the most useful testing environment among those discussed in this paper. FIT IoT-LAB can also help researchers and all those who are interested in IIoT cybersecurity research and development to visualize

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)
Issues (49) 2021
ISSN: 2616-9185
www.mecsj.com

their research through the visual simulator available in the lab. The lab was equipped with different types of hardware and software that can serve a wide range of research and experiments. Testbed lactation is also an important factor in IIoT tests; therefore, FIT IoT-LAB is situated in different geographic locations in more than one country, so users can test different networks and IIoT node clusters. The lab was very easy to sign up for and access instantly as long as the user had an official email account for an educational institution or research center. Thus, no additional approval by lab admins is needed. On the other hand, the iTrust lab has one more useful advantage that is not available in FIT IoT-LAB, which is its integration with other ICS labs, as iTrust has three ICS labs, each focusing on a specific area of ICS cybersecurity research. However, as FIT IoT-LAB has an API interface, so users can extend the outcomes of research conducted in this lab to other labs for further exploring and testing.

Conclusion

ICS and new Industry 4.0 technology, such as IIoT, are advanced and complex systems that need sophisticated equipment and tools. Building a development environment and testbeds requires a budget and efforts that small educational institutions and research centers simply cannot afford. The increasing number of cyberattacks and threats in current times drives

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)
Issues (49) 2021
ISSN: 2616-9185
www.mecsj.com

the need for more workforce development and research. Although the open ICS testbeds explored herein are good options for students and researchers, they are not enough to address the prevailing shortage in ICS cybersecurity testbeds. In my opinion, there are two ways to help bridge this gap existing in terms of testbeds and research facilities. First, governments and leading tech corporations must fulfill their role in supporting educational institutions and researchers by providing free or affordable testbeds to enhance ICS cybersecurity studies and research. Second, the partnerships between universities and research centers to share these resources with educational institutions and research centers can help address the shortage, and this would also reflect enhanced research quality and quantity. The OneLab consortium initiative in Europe, which brings together research centers from different countries, is a great example of how partnerships can boost research and workforce development. Finally, it will be useful if all current open testbeds adopt the API interfaces so that researchers can extend the outcomes to other free testing environments for greater testing and research.

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)
Issues (49) 2021
ISSN: 2616-9185
www.mecsj.com

References

Ackerman, P. (2017). Industrial Cybersecurity: Efficiently secure critical infrastructure systems. Packt Publishing Ltd.

Adjih, C., Baccelli, E., Fleury, E., Harter, G., Mitton, N., Noel, T., ... & Watteyne, T. (2015, December). FIT IoT-LAB: A large scale open experimental IoT testbed. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)* (pp. 459-464). IEEE.

Bellavista, P., & Zanni, A. (2016, September). Towards better scalability for IoT-cloud interactions via combined exploitation of MQTT and CoAP. In 2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI) (pp. 1-6). IEEE.

Drias, Z., Serhrouchni, A., & Vogel, O. (2015, July). Taxonomy of attacks on industrial control protocols. In *2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS)* (pp. 1-6). IEEE.

Fambon, O., Fleury, E., Harter, G., Pissard-Gibollet, R., & Saint-Marcel, F. (2014). FIT IoT-LAB tutorial: hands-on practice with a very large scale testbed tool for the Internet of Things. 10èmes journées francophones Mobilité et Ubiquité, UbiMob2014.

Feng, C., Li, T., & Chana, D. (2017, June). Multi-level anomaly detection in industrial control systems via package signatures and LSTM networks. In *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)* (pp. 261-272). IEEE.

Fleury, E., Mitton, N., Noel, T., & Adjih, C. (2015). Fit iot-lab: The largest iot open experimental testbed. *Ercim News*, (101), 4.

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)
Issues (49) 2021
ISSN: 2616-9185
www.mecsj.com

Green, B., Derbyshire, R., Knowles, W., Boorman, J., Ciholas, P., Prince, D., & Hutchison, D. (2020). {ICS} Testbed Tetris: Practical Building Blocks Towards a Cyber Security Resource. In *13th {USENIX} Workshop on Cyber Security Experimentation and Test ({CSET} 20)*.

Hankin, C., Chana, D., Green, B., Khan, R., Peter M3., Popov, P., Rashid, A., & Sezer, S. (2018) Open Testbeds for CNI. Imperial College London.

Harter, G., Pissard-Gibollet, R., Saint-Marcel, F., Schreiner, G., & Vandaele, J. (2015, September). FIT IoT-LABA: Large Scale Open Experimental IoT Testbed. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking* (pp. 176-178).

Hunkeler, U., Truong, H. L., & Stanford-Clark, A. (2008, January). MQTT-S—A publish/subscribe protocol for Wireless Sensor Networks. In 2008 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE'08) (pp. 791-798). IEEE.

Kim, B. K., Kang, D. H., Na, J. C., & Chung, T. M. (2016, January). Abnormal traffic filtering mechanism for protecting ICS networks. In *2016 18th International Conference on Advanced Communication Technology (ICACT)* (pp. 436-440). IEEE.

McBride, S., Schou, C., & Slay, J. (September, 2020) A Security Workforce to Bridge the IT-OT Gap. Industrial Cybersecurity Workforce Development. Idaho State University.

Murray, G., Johnstone, M. N., & Valli, C. (2017). The convergence of IT and OT in critical infrastructure.

Shin, I. (2017). A novel abnormal behavior detection framework to maximize the availability in Smart Grid. *Smart Media Journal*, *6*(3), 95-102.

Siboni, S., Sachidananda, V., Meidan, Y., Bohadana, M., Mathov, Y., Bhairav, S., ... & Elovici, Y. (2019). Security testbed for Internet-of-Things devices. *IEEE transactions on reliability*, *68*(1), 23-44.

University of Southern California. (n.d.). *Tutornet: A low power Wireless IoT Testbed*. Autonomous Networks Research Group. http://anrg.usc.edu/www/tutornet/.

Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)
Issues (49) 2021
ISSN: 2616-9185
www.mecsj.com

Viterbi (n.d.) Tutornet: A Low Power Wireless IoT Testbed. the Viterbi School of Engineering at the University of Southern California. Retrieved from: https://cci.usc.edu/index.php/research/testbeds