This article has been published in:
S. Kucek and M. Leitner, “Training the Human-in-the-Loop in Industrial Cyber Ranges,” in Digital Transformation in Semiconductor Manufacturing, Cham, 2020, pp. 107–118, http://dx.doi.org/10.1007/978-3-030-48602-0_10

1st European Advances in Digitization Conference

Training the Human-in-the-Loop in Industrial Cyber Ranges

Stela Kucek, Maria Leitner

AIT Austrian Institute of Technology, Center for Digital Safety & Security

stela.kucek.fl@ait.ac.at

maria.leitner@ait.ac.at

Abstract

With the trend of automation in manufacturing and the advancements of technologies, knowledge, skills and abilities of the workforce should develop accordingly. Current training technologies often do not provide hands-on training and exercises. Hence, training methods and technologies need to adapt to support the new requirements and progress. Cyber ranges are virtual environments that mimic realistic networks and systems and can be used for e.g., training, exercises or research. While current state of the art focuses mostly on technical designs and developments, this paper focuses on assessing and integrating the human-in-the-loop in industrial cyber ranges (i.e. cyber ranges with specific scenarios that can be found in Industry 4.0, manufacturing or related topics). We describe the human-in-the-loop in cyber ranges and outline an example application scenario. Furthermore, we discuss challenges in relation to the implementation in cyber ranges. For future work, we will utilize this design and development scheme for further advancements of industrial cyber ranges and its components.

1. Introduction

With digitization in industry and the shift towards smart manufacturing, industrial control systems (ICS) and their interconnectedness has increased the likelihood of potential attacks. In recent years, attacks such as *Stuxnet* or *Crashoverride* have demonstrated that security is a key factor in ICS. Waslo et al. (Waslo et al., 2017) state that enhancing digital capabilities in the production and supply chain processes can lead to new cyber risks. For example, exploiting SCADA (Supervisory control and data acquisition) system vulnerabilities may be a potential threat (Ralston et al., 2007).

However, organizations in many domains such as manufacturing, energy, or logistics are facing the challenges with the increased speed of evolving threats and vulnerabilities as well as preventing, detecting and mitigating (cyber) security incidents. The aim of many organizations is to increase their resilience by increasing their preparedness and response times of (cyber) incidents. When an unexpected or unwanted event (i.e. incident) occurs in a highly automated environment, the responsible human operator should be able to react in a fast and efficient manner. For this fast and efficient response, new training methods need to be assessed to enable dynamic, real-time training and exercises. In fact, Weyer et al. (Weyer et al., 2015) state that new teaching and training platforms have to be developed in order to train and support new qualifications in cyber-physical systems (CPS) (often also referred to as Industry 4.0 – the fourth industrial revolution). These new platforms would support the adequate training and preparation of employees (from administrative staff, engineers, computer security incident response (CSIRT) teams to the management board) to increase security awareness and skills as well as providing novel approaches to capability management in organizations. This would support organizations, as they often provide inhouse training to increase the skills and abilities of the workforce as it is in general challenging to find highly-skilled workers (see (Neuman, 2009)). Current training methods support only rarely realistic simulations of the business operations, technology and their impact (e.g., e-learning).

In this paper, we introduce cyber ranges as a training platform to the manufacturing domain in order to support the aforementioned new qualifications and challenges. The NIST (National Institute of Standards and Technology, U.S. Department of Commerce, 2018) specifies *cyber ranges as interactive, simulated representations of an organization’s network, system tools, and applications that are*

connected to a simulated Internet level environment. Hence, cyber ranges can simulate information technology (IT) and operational technology (OT) infrastructures, benign and malicious users as well as (cyber) incidents (Frank et al., 2017). On top of these virtual environments, training scenarios are practiced (Davis and Margath, 2013; Pham et al., 2016). The advantage is that this hands-on training is conducted in a safe environment and not the production systems. In the context of cyber-physical systems in manufacturing, cyber ranges can be utilized to train a target audience e.g., to operate an infrastructure, to practice relevant procedures, as well as to handle security-related incidents. In this paper, we aim to describe how cyber ranges can be adapted for training and exercises in manufacturing incorporating the human-in-the-loop.

Therefore, we review current trends and aspirations in technical training and exercises in manufacturing and introduce cyber ranges as a technology platform for training and exercises. With this, organizations may enable hands-on training for employees (e.g., engineers, incident response teams, managers, etc.). This training enables more practice than usual training situations (e.g., lecturers or e-learning) and supports the training of technical (e.g., knowhow and practice of networks and systems) and organizational topics (e.g., contingency processes or hierarchical structures). The advantages of using virtual environments are not only the flexibility and reusability of scenarios but also that training can be conducted anywhere (using an Internet-enabled environment). Hence, training can be conducted on premises but also with virtual and distributed teams. Based on current state of the art, we describe cyber ranges and potential application areas and introduce the human-in-the-loop concept. Furthermore, we outline an application scenario that showcases the concept of the human-in-the-loop in cyber ranges. We discuss current challenges for the implementation and evaluation in cyber ranges.

The rest of this paper is structured as follows: Section 2 outlines related work and background on cyber ranges, training technologies in manufacturing and the human-in-the-loop. Section 3 introduces cyber ranges and their applications. In Section 4, the human-in-the-loop is described within industrial cyber ranges. Section 5 presents an example scenario that demonstrates the concept. Section 6 discusses the content and implications of the approach and concludes the paper.

2. Related Work

Cyber security management has become very important in ICS, for example Knowles et al (Knowles et al., 2015) provide a review of cyber security management in ICS. Fabro et al. (Fabro et al., 2016) suggest that one of the five key countermeasures of ICS security is to *manage the human.* This includes to provide ICS security training for all operators and administrators. As this paper centers on training technologies, we briefly review technical hands-on training methodologies and technologies in the context of CPS and cyber ranges and do not focus on e-learning, augmented or virtual reality approaches. Weyer et al. (Weyer et al., 2015) state that there is a need for new teaching and training platforms due to the need of new qualifications in Industry 4.0. This can be seen in the recent developments.

Physical environments: Learning factories

Schallock et al. (Schallock et al., 2018) describe a design of a learning factory that focuses not only on technical skills, but also trains decision making, group work and performance monitoring skills of the production staff. They present a conceptual design that encompasses theoretical, as well as practical aspects applied in a German learning factory. Simons et al. (Simons et al., 2017) propose a similar concept, namely a holistic, fully automated Industry 4.0 learning factory. These works provide a physical environment (or single physical devices such as PLCs and robots) to demonstrate and train production processes and not a virtual environment such as provided with cyber ranges or other virtual testbeds.

Virtual environments: ICS testbeds and cyber ranges

Research and industry has developed virtual environments for training and experimentation in ICS. Holm et al. (Holm et al., 2015) provide a systematic review of 30 ICS testbeds. Common methods for implementing such environments: are hardware, simulation, emulation and virtualization (Holm et al., 2015). Typical testbed components are the control center, communication architecture, field devices, and the physical process. The authors suggest using taxonomies to make ICS testbeds more tangible and

comparable. Common objectives are to enable vulnerability analysis, education and tests of defense mechanisms (compare (Siddiqi et al., 2018)). While the work of (Holm et al., 2015) is on systemizing and categorizing ICS testbeds. In this paper, we formulate and integrate a human-in-the-loop concept for industrial cyber ranges.

Cyber ranges are virtual environments that simulate or mimic IT and OT systems and networks. Many cyber ranges are used in the public domain for research, training, exercises and a review of cyber ranges can be found in (Davis and Magrath, 2013). Cyber ranges do not automatically include ICS, however, many of the cyber ranges started to integrate components or subsystems that represent OT. Please refer to Section 3 for more information on cyber ranges.
Note that in practice other approaches to training for ICS exists, but either use different technologies (physical devices, virtual reality) or have a different goal (education, technical testing of the system, evaluating low-level processes).

The Human-in-the-Loop Concept

The concept of a "*human-in-the-loop*" (HitL) has been a well-known principle, representing a model where the interaction of a human actor is required (Karwowski, 2006). Its application can be found in well-known examples such as flight or marine simulators. Recently, its application can be found in many other domains such as aviation automation (Bilimoria et al., 2018), system design and modeling (Smith et al., 2018), virtual reality (Sherman and Craig, 2018) and machine learning (Warrier and Devasia, 2017). The HitL has been also introduced to cyber-physical systems in (Schirner et al., 2013) where body or brain sensors interact with an embedded system and a physical environment. Stouffer et al (Stouffer et al., 2014) suggest that the HitL concept can be used as a form of control and supervision of the system rather than only automated supervision in ICS. This includes also manual modes of ICS where humans completely control the systems (opposite to open-loop or closed-loop control systems). As a typical ICS contains numerous control loops, human intervention and supervision may be required and a specific skillset for the interaction with these systems. Hence, this mix of control systems might bring a new perspective to training incorporating the semi-automated control systems that require human supervision and interaction. This would align witih Weyer et al. (Weyer et al., 2015) and their proposed need for new qualifications in smart manufacturing. In addition, with the HitL concept, we aim to address the significance of a human operator in ICSs, as well as their competences and skills required in this context.

Hence, this brief review of related work displays that there is a need for dynamic and hands-on training in cyber security in ICS and a vivid research on environments that support various purposes such as education, training or research. While many of these papers focus on the design and development of infrastructures, to the best of our knowledge, none of the papers integrate the human-in-the-loop in these systems. Surprisingly, we also found little or no literature on the concept of hands-on technical exercises in cyber ranges in manufacturing. However, dynamic exercises will become more essential particularly with coping daily or unexpected situations (e.g., cyber incidents).

3. Cyber Ranges for Smart Manufacturing

In general, cyber ranges are virtual environments that simulate systems and critical (cyber) security incidents on these systems. Cyber ranges can simulate various technologies such as IT and OT infrastructures. They have been widely used in cyber security training and education, cyber security competitions and challenges, national cyber security exercises and more (Davis and Magrath, 2013). In addition to existing ICS testbeds (see Section 2), many cyber ranges integrate ICS components as part of a larger and complex systems and to mimic various attack vectors. Hence, ICS testbeds may overlap or be part of cyber ranges. Furthermore, realistic scenarios are simulated on top of these environments, this can include multiple aspects such as benign and malicious users, network traffic, external stakeholders or sites, security incidents and more. Figure 1 displays a general scheme of components of cyber ranges. However, each individual cyber range may have a similar or different configuration. It can be seen from the figure that there is a simulated infrastructure of networks and systems, supported processes or contingency plans, simulated stakeholders, simulated external sites and participants (blue

and red teams). The blue teams can be for example the trainees of a training and the red team can be also trainees who aim to infiltrate the system (or could be replaced with a program).

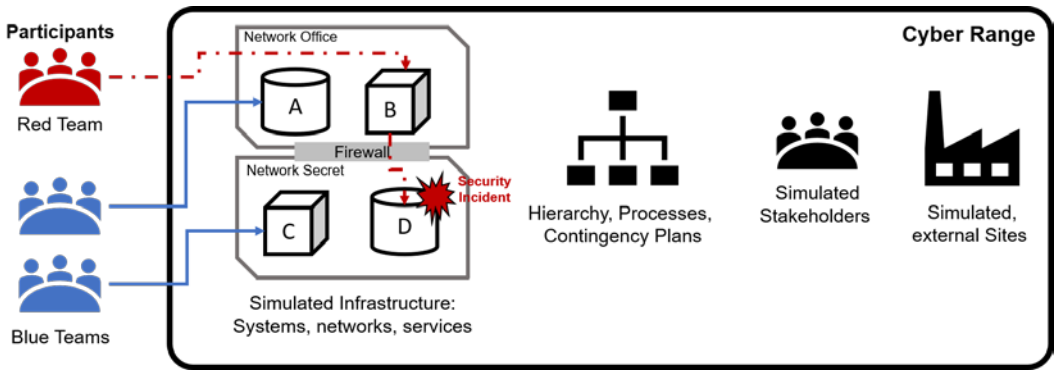

Figure 1 Cyber range schema

This setup allows for manifold activities to conduct on, the two most common activities are currently:

- *Training and exercises*: Cyber ranges can provide a multidimensional way of training cyber security or information security staff and general staff. In particular, this hands-on training is heavily requested by organizations (Frank et al., 2017) for cyber security staff. In addition, training and exercises on cyber ranges allow for dynamic situations, like the real world. Training supports security awareness trainings but also technical trainings and exercises. In manufacturing this could be e.g., training daily or rare situations of business operations.
- *Research and experimentation*: Cyber ranges support experimentation and testing of software, hardware, as well as human reactions and therefore can be used in research. Many cyber ranges have been developed that have this background (see e.g., (Davis and Magrath, 2013)). For example, the virtualization of certain automation processing components (and their impact on production in case of incidents) or the handling of stressful situations could be reviewed in cyber ranges.

The advantage to use a cyber range is that situations and strategies can be tested within a safe and isolated virtual environment and the outcome does not affect production. Also, the environment allows a lot of practice allowing theory to be manifested with practical and hands-on work. The cyber range approach can be applied and adapted to any industrial domain e.g., from water supply, logistics, energy to manufacturing. Hence, in cyber-physical systems, cyber ranges can be utilized to e.g., exercise contingency plans in case of security incidents, operating infrastructures, testing relevant procedures and others. They may be further called "*industrial cyber ranges*" as they might have specifics and scenarios focusing only on smart manufacturing and related challenges.

4. The Human-in-the-Loop in Cyber Ranges

In this section, we aim to describe a new concept for training and building a capable and highly skilled workforce in Industry 4.0. The core of this idea is to simulate real situations in a safe environment with the use of user- and skill-specific scenarios in the context of modern industry. We have introduced cyber ranges and their application in Section 3. An industrial cyber range can be composed of virtual components that represent IT and OT infrastructures. Apart from the system itself, there is a human actor (further called *participant*) interacting with the system, in the industrial context often referred to as an *operator (or engineer)*, and a participant can be a single person or a team. They can be part of various target groups: from manufacturing engineers, control engineers to the shift managers and managers on duty. Applying the HitL principle to industrial cyber ranges, the focus shifts to the operators or engineers and their interaction with the system. In fact, in the training within an industrial cyber range, each trainee or participant is a *human-in-the-loop*.

The interaction is typically enabled within a scenario. For example, the participant can be confronted with situations that reflect daily business routines but also rare situations (e.g., cyber incident response, cyber attacks, production shutdowns, etc.). Within these scenarios, operators are performing their routine tasks or processes such as interactions with ICS components and machines, communication with other (distributed) teams, review of news and monitoring of controls. The human-in-the-loop with all these interactions is depicted in Figure 2.

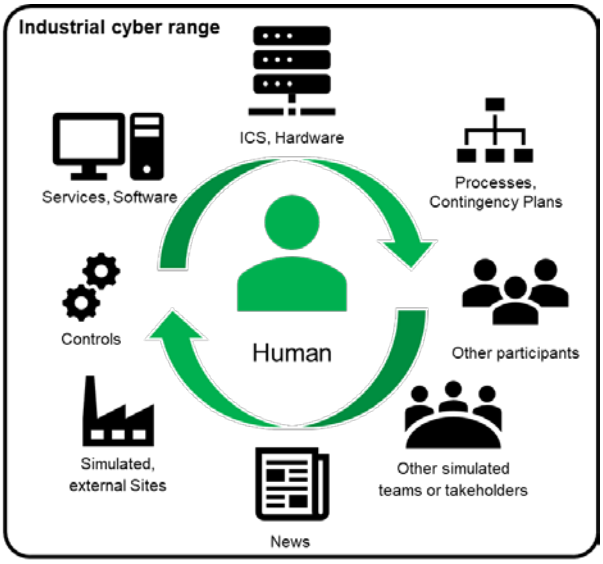

Figure 2 Human-in-the-loop in industrial cyber ranges

It can be seen from Figure 2 that the participant is the central point of all actions. All interactions with the cyber range such as with other participants, other simulated actors, controls, ICS and others revolve around the participant.

In a cyber security training or exercise, the participant interacts with the cyber range to manage certain situations. A typical training could e.g., focus on improving reaction times, assessing the quality of decision making and dealing with unwanted or unexpected situations. We outline an example of a scenario for the case of manufacturing in the following section.

5. Application Scenario

This section sketches a (fictive) example scenario that demonstrates how training on the cyber range can be designed. A scenario is a situation where participants need to handle business operations. The participants use the systems and interfaces provided in the cyber range to resolve the situation following regular business standards and procedures. The actions performed by the participant are to be observed and later evaluated. Example scenarios are the failure of one or more critical system components, denial of service, social engineering, and malicious code exploitation (Falco et al., 2002; Tuptuk and Hailes, 2018). The following fictive example is based within the manufacturing domain but can also occur in other domains where the same technology is utilized.

Background

In this scenario, a control system of the robot arm is manipulated from a source that has access to the control device of the robot or the monitoring device communicating with the control system. This scenario stems from examples of potential vulnerabilities of automation systems such as outlined in (ICS-CERT, 2018, 2015). In this scenario, the relevant parameters passed to the control device of the robot are incorrect, i.e. the diameter of the coating does not match the size of the semiconductor material currently processed by the robot. As a result, the semiconductor robot misplaces the coating on the semiconductor material which may have a high impact on the production. Potential consequences of this incident are e.g., faulty semiconductor material, overflow of the coating material or damaged surfaces.

Setup

The goal of this scenario is for the trainee to rehearse an incident handling protocol in case of identified manipulations of an automation component, i.e. robot arm handling semiconductor material. The trainee of our scenario is a control engineer (ENG) who is supervising the automation process via software on their workstation in a fictive organization. The ENGs main task is to manage the incident scenario (described above). Apart from the ENG, there are several roles that act as supporting roles to the ENG. One of them is a local operator team (LOT), i.e. engineers working nearby with physical access to the robot. Next, there is an incident management and response (INC) team that the ENG can contact for technical support and incidents. Lastly, the manager on duty (MOD) is a shift manager.

Script

The scenario is planned by using a script that consists of the time line and the associated steps to be performed by the participants (see Table 1). It can be seen from the table that the ENG must perform many steps throughout the scenario to assess the situation, investigate the incident and resolve the incident. INC, MOD and LOT can be simulated stakeholders or active participants in this scenario.

Table 1 Scenario script

Roles	Steps
ENG	1. Identifies unexpected, abnormal behavior of the ICS component on the ENG workstation.
ENG	2. Stops or pauses the ICS component. 2.1. The controls (i.e., start, stop, pause) and parameters for the arm movement are provided on the ENG workstation interface. ENG uses the provided controls; presses the STOP button to prevent further damage. 2.2. The system does not respond to the termination attempts from the interface. ENG informs a MOD. ENG requests a LOT that is close to the location of the incident for assistance. 2.3. No LOTs are available, the ENG terminates the arm physically (e.g., by switching off the hardware or unplugging).
ENG	3. Reports the incident to INC and MOD. Documents the circumstances and consequences of incident, measures taken, and status of situation. Sends information to INC.
INC	4. Analyzes incident and responds with feedback. There is a defined incident response protocol for the incident. INC sends the recovery steps to the ENG: (1) Assuming the robot arm is off, first identify misconfigured parameters and correct them. (2) Check the default parameters for correctness. (3) Perform a malware scan of the control-monitor software to detect a malicious program if present. (4) If malware was found, respond in the same thread of the initial report and the issue will be forwarded or solved by the support team. (5) If no malware was found, start the robot arm again, but monitor continuously to determine if the issue persists. (6) If the issue persists, respond in the same thread of the initial report and the issue will be forwarded to the support team.
ENG	5. Performs steps provided in the INC feedback and responds with required details that were missing in the initial report

Implementation in the Cyber Range

The implementation in the cyber range is challenging as many ICS technologies have not been virtualized and therefore, many testbeds develop simulations or emulations to simulate the industrial process or the field devices that are related to it (see e.g., (Holm et al., 2015)). Therefore, we plan to simulate the workstations for ENG using a control monitor interface of the handling robot and for INC and MOD as shown in Figure 3. Figure 3 displays the simplified architectural scheme of the scenario. More components such as field devices, control stations, etc. could be integrated in order to make the scenario more realistic. It can be seen from the figure that the ENG workstation is connected to the control center that transmits the ongoing status to the ENG workstation. Furthermore, the control center is connected to the ICS component 1 (e.g., a programmable logic controller, PLC) that mimics the behavior of such an automation processing system (compare smart factory[1] visualizations for example).

[1] http://www.starteasy.io/ (last access on January 30, 2019)

Additional network communications or connections, even though not outlined in the scheme, are imaginable and would contribute to the realism of the scenario. All communication between participants is conducted by email and telephone.

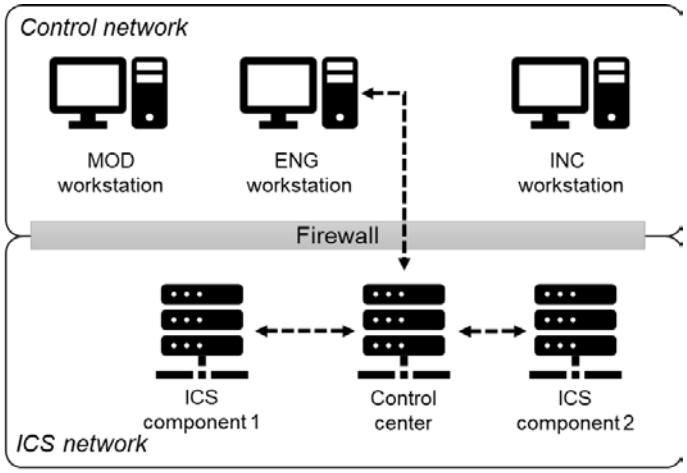

Figure 3 Simplified scheme of example environment

6. Discussion and Conclusions

Training on a cyber range enables the participants to gain capabilities, to practice new, established or changed routines, as well as to test and evaluate processes and procedures in a safe and isolated environment. Even if the participant does not need to apply the gained skills in daily business, the hands-on training will raise awareness and increase the preparedness of participants for these situations. Hence, when these situations occur, participants may react more goal-oriented and efficiently and therefore unwanted situations may be quicker resolved.

One big challenge for cyber ranges and ICS testbeds is the virtualization and simulation of the manufacturing environment. As stated in (Holm et al., 2015), only some technologies have been virtualized and only a few are gradually virtualized to testbeds. Hence, it would be helpful if vendors and others consider providing simulation models or virtualized technologies for research purposes. Another challenge is the simulation of the field devices and physical process itself (Holm et al., 2015). The utilization of certain devices and process depends heavily on the application scenario (and the defined purpose and goals). In each scenario, designers would have to evaluate if the simulation of field devices or the physical process is really required to support the goals of the training.

Another challenge is the measurement and evaluation of (1) the success of training and exercises, (2) the team performance, (3) the individual participant's performance and (4) the scenario and technology utilized in the cyber range. This is particularly interesting when using different systems and networks in different scenarios. First examples for the evaluation of cyber exercises exist (Schepens et al., 2002). More research needs to adequately assess evaluation measures and procedures for technical trainings.

In conclusion, the utilization of cyber ranges as training environments to prepare employees for regular and unexpected challenges of business operations is a well-established platform in the cyber security domain. In this paper, we introduced industrial cyber ranges and the integration of the human-in-the-loop. With this, we emphasize on the individual human operator in (manufacturing) systems and the importance of human-machine interactions. We described an application scenario in the semiconductor industry to highlight how the human is the central point of communication and how many activities are conducted in such a hands-on training. With this dynamic and real-time training, we aim to achieve highly-skilled teams that can manage various situations, handle relevant systems, and cope with potential failures. This contributes to the resilience of organizations. For future work, we will use this concept as a basis for designing and implementing a manufacturing use case in the cyber range. After implementation, we plan to evaluate the use case with practical hands-on sessions.

References

Bilimoria, K.D., Hayashi, M., Sheth, K., 2018. Human-in-the-Loop Evaluation of Dynamic Multi-Flight Common Route Advisories. In: 2018 Aviation Technology, Integration, and Operations Conference, AIAA AVIATION Forum. American Institute of Aeronautics and Astronautics.

Davis, J., Margath, S., 2013. A Survey of Cyber Ranges and Testbeds (No. DSTO-GD-0771). Cyber Electronic Warfare Division, DSTO Defence Science and Technology Organisation, Edinburgh, South Australia 5111, Australia.

Fabro, M., Gorski, E., Spiers, N., Diedrich, J., Kuipers, D., 2016. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. Department of Homeland Security's NCCIS and ICS-CERT.

Falco, J., Wavering, A., Proctor, F., 2002. IT security for industrial control systems (No. NIST IR 6859). National Institute of Standards and Technology, Gaithersburg, MD.

Frank, M., Leitner, M., Pahi, T., 2017. Design Considerations for Cyber Security Testbeds: A Case Study on a Cyber Security Testbed for Education. In: IEEE 3rd Intl Conf on Cyber Science and Technology Congress(CyberSciTech). Presented at the CyberSciTech, IEEE, Orlando, Florida, pp. 38–46.

Holm, H., Karresand, M., Vidström, A., Westring, E., 2015. A Survey of Industrial Control System Testbeds. In: Buchegger, S., Dam, M. (Eds.), Secure IT Systems, Lecture Notes in Computer Science. Springer International Publishing, pp. 11–26.

ICS-CERT, 2015. Rockwell Automation 1766-L32 Series Vulnerability [WWW Document]. URL https://ics-cert.us-cert.gov/alerts/ICS-ALERT-15-225-02A (accessed 1.29.19).

ICS-CERT, 2018. Omron CX-One [WWW Document]. URL https://ics-cert.us-cert.gov/advisories/ICSA-18-338-01 (accessed 1.29.19).

Karwowski, W., 2006. International Encyclopedia of Ergonomics and Human Factors, Second Edition - 3 Volume Set. CRC Press.

Knowles, W., Prince, D., Hutchison, D., Disso, J.F.P., Jones, K., 2015. A survey of cyber security management in industrial control systems. Int. J. Crit. Infrastruct. Prot. 9, 52–80.

National Institute of Standards and Technology, U.S. Department of Commerce, 2018. Cyber Ranges. National Institute of Standards and Technology, US.

Neuman, C., 2009. Challenges in security for cyber-physical systems. In: DHS Workshop on Future Directions in Cyber-Physical Systems Security. Citeseer, pp. 22–24.

Pham, C., Tang, D., Chinen, K., Beuran, R., 2016. CyRIS: A Cyber Range Instantiation System for Facilitating Security Training. In: Proceedings of the Seventh Symposium on Information and Communication Technology, SoICT '16. ACM, New York, NY, USA, pp. 251–258.

Ralston, P.A.S., Graham, J.H., Hieb, J.L., 2007. Cyber security risk assessment for SCADA and DCS networks. ISA Trans. 46, 583–594.

Schallock, B., Rybski, C., Jochem, R., Kohl, H., 2018. Learning Factory for Industry 4.0 to provide future skills beyond technical training. Procedia Manuf., "Advanced Engineering Education & Training for Manufacturing Innovation"8th CIRP Sponsored Conference on Learning Factories (CLF 2018) 23, 27–32.

Schepens, W.J., Ragsdale, D.J., Surdu, J.R., Schafer, J., New Port, R., 2002. The Cyber Defense Exercise: An evaluation of the effectiveness of information assurance education. J. Inf. Secur. 1, 1–14.

Schirner, G., Erdogmus, D., Chowdhury, K., Padir, T., 2013. The Future of Human-in-the-Loop Cyber-Physical Systems. Computer 46, 36–45.

Sherman, W.R., Craig, A.B., 2018. Chapter 3 - The Human in the Loop. In: Sherman, W.R., Craig, A.B. (Eds.), Understanding Virtual Reality (Second Edition), The Morgan Kaufmann Series in Computer Graphics. Morgan Kaufmann, Boston, pp. 108–188.

Siddiqi, A., Tippenhauer, N.O., Mashima, D., Chen, B., 2018. On Practical Threat Scenario Testing in an Electric Power ICS Testbed. In: Proceedings of the 4th ACM Workshop on Cyber-Physical System Security, CPSS '18. ACM, New York, NY, USA, pp. 15–21.

Simons, S., Abé, P., Neser, S., 2017. Learning in the AutFab – The Fully Automated Industrie 4.0 Learning Factory of the University of Applied Sciences Darmstadt. Procedia Manuf., 7th Conference on Learning Factories, CLF 2017 9, 81–88.

Smith, A., Kumar, V., Boyd-Graber, J., Seppi, K., Findlater, L., 2018. Closing the Loop: User-Centered Design and Evaluation of a Human-in-the-Loop Topic Modeling System. In: 23rd International Conference on Intelligent User Interfaces, IUI '18. ACM, New York, NY, USA, pp. 293–304.

Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., Hahn, A., 2014. Guide to Industrial Control Systems (ICS) Security. NIST Spec. Publ. 255.

Tuptuk, N., Hailes, S., 2018. Security of smart manufacturing systems. J. Manuf. Syst. 47, 93–106.

Warrier, R.B., Devasia, S., 2017. Data-based Iterative Human-in-the-loop Robot-Learning for Output Tracking. IFAC-Pap., 20th IFAC World Congress 50, 12113–12118.

Waslo, R., Lewis, T., Hajj, R., Carton, R., 2017. Industry 4.0 and cybersecurity. Deloitte Insights.

Weyer, S., Schmitt, M., Ohmer, M., Gorecky, D., 2015. Towards Industry 4.0 - Standardization as the crucial challenge for highly modular, multi-vendor production systems. IFAC-Pap., 15th IFAC Symposium on Information Control Problems in Manufacturing 48, 579–584.