Electronic Communications of the EASST
Volume 079 (2020)

Interactive Workshop
on the Industrial Application of Verification and Testing
ETAPS 2020 Workshop
(InterAVT 2020)

CYBERWISER.eu: Innovative Cyber Range Platform for Cybersecurity Training in Industrial Systems

Mariano Basile, Gianluca Dini and Dario Varano

8 Pages

Guest Editors: Stylianos Basagiannis, Goetz Botterweck, Anila Mjeda
ECEASST Home Page: http://www.easst.org/eceasst/ ISSN 1863-2122

CYBERWISER.eu: Innovative Cyber Range Platform for Cybersecurity Training in Industrial Systems

Mariano Basile, Gianluca Dini and Dario Varano

Dept. of Computer Engineering
University of Pisa
Pisa (PI), Italy
[name].[surname]@unipi.it

Abstract: Information technologies are nowadays part of industrial systems. Employees in charge of managing these systems typically have little or very little knowledge of cybersecurity. In this work we initially explore the challenges related to cybersecurity training in industrial systems and then we propose an approach based on CYBERWISER.eu cyber range platform. A cyber range provides a multipurpose virtual environment in which organisations can test critical capabilities and reveal how effectively they integrate people, processes, and technology to protect their strategic information, services, and assets. By facilitating high-fidelity simulations, a cyber range can associate the cybersecurity training phase with a personalized security testing, together with a unit testing, on different kind of systems, including SCADA.

Keywords: training, cybersecurity, security testing, unit testing, cyber range, cyber-attacks, cyber threat, cyber-physical system, cyberwiser

1 Introduction

With the increasing dependency on Information Technology (IT) systems, any business from any sector is facing cyber risks. This includes industrial systems, where cyber risks nowadays reach dramatic levels. Furthermore, the request for an evolution in industrial development, together with the introduction of the Industry 4.0 paradigm, paves the way for new categories of cyber threats [1][2]. For these reasons, the need to count on highly skilled, multi-disciplined, cybersecurity professionals are more urgent than ever[3]. In 2019, 65% of organizations had a shortage of staff dedicated to cybersecurity. That lack of skilled and experienced cybersecurity personnel is the top concern among survey respondents. In addition, 51% of cybersecurity professionals stated that their organization is at moderate or extreme risk due to cybersecurity staff shortage. Nevertheless, industries struggle to consider cybersecurity as a requirement. This lead either to a complete lack of cybersecurity training or, in few cases, to the lack of effective training. Additionally, the security testing of industrial systems usually can be done following two different approach. One approach is to have an accurate hardware replica of the plant. This can also be represented on a lower scale and must be isolated from the external world. This approach is instead the most *effective*. Indeed, trainees can check the impact of a cyber-attack on real devices. On the other hand, such an approach is expensive due to the costs for hardware acquisition and maintenance.

An alternative approach consists in virtualizing the plant. This includes, but it is not limited to, virtualization of the industry systems available in the plant, the software running on these systems, and the network infrastructure and configuration. The virtualized environment is also placed in a sandbox where external elements cannot intervene. This approach is the most *efficient*, as it can be quickly reconfigured and does not need additional hardware resources. The main drawback is the effectiveness of the training, as the impact of a cyber-attack cannot be accurately reported on a software instance. Additionally, such software needs to be maintained over time.

The paper provides a threefold contribution. First, we explore the challenges related to cybersecurity training in industrial systems. Secondly, we propose an approach for associating the cybersecurity training with security testing and unit testing. Finally, we propose the CYBERWISER.eu cyber range platform as a unified to cybersecurity training and testing in industrial ICT environments [4]. The complexity of industrial systems and the limitations imposed by using associated software/hardware models make the task of training personnel rather complicated and ineffective. Additionally, having a customized environment to conduct tests of realistic components is an awkward task. In this regard, the CYBERWISER.eu platform is an innovative cyber range aimed at providing a virtualized environment where realistic cybersecurity training scenarios can be designed. Such an environment can be either fully or partially virtualized, i.e. making use of existing physical devices. The aim of a cyber range is to provide training and testing skills for cybersecurity professionals [5]. Several cyber range platforms have been proposed in the literature, including [6] and [17]–[19]. The most relevant players in the cyber training sector are usually evaluated along two different dimensions: i) the breadth of product offering, i.e. certification only, training courses, cyber range and cyber range + training courses; ii) key target market, i.e. individuals, private companies, public administration and strategic/military infrastructures. The CYBERWISER.eu platform offers a cyber range + training courses product and it is mainly directed to both individuals and private companies.

In the context of CYBERWISER.eu, a *training scenario* consists of a set of virtual resources representing the ICT infrastructure of an organization (e.g., a company), or a portion of it. Training scenarios give the chance to perform cybersecurity training exercises, simulating cyber-attacks and defence mechanisms, monitoring exercises progress and real-time assessment of user performance.

The rest of the paper is organized as follows. In Section 2 we introduce the water tank case study which constitutes a leading example throughout the paper. The water tank is a simple yet effective example of a real industrial cyber-physical system along with its cyber-attacks that allows us to give an immediate and clear example of the proposed methodology. In Section 3 we discuss cybersecurity training and testing challenges in industrial systems, taking as reference the water tank case study. In Section 4 we present an overview of the CYBERWISER.eu platform. In Section 5 we explain how CYBERWISER.eu can be exploited in order to address these challenges. Finally, Section 6 concludes the paper.

2 Case study: The Water Tank

For illustration purposes we consider a simple yet meaningful case study, namely the water tank. This is a well-known example in control theory. Several versions of this case study are available in the literature. In this paper, the one described in [7] is considered. A formal verification of the safety properties related to the water tank nonlinear control system can be found in [8]. *Figure 1* shows the water tank. In this system:

- The water arrives at a variable rate w_i through an input pipe;

- The water leaves through an output pipe in the tank base at a rate w_o controlled by a *valve*;
- The valve position is given by $v \in [0,1]$ (0 and 1 modelling respectively the fact that the valve is closed or open). The initial position, at time $t = 0$, of the valve is equal to some constant $v\ (0) = V_0$;
- The maximal throughput capacity of the output pipe is *C*. Therefore, its actual throughput at each moment is *C v*.
- The valve is controlled by a *sensor* measuring the level *l* of water in the tank. The sensor aims at keeping this level in a given interval $[L_1, L_2]$;

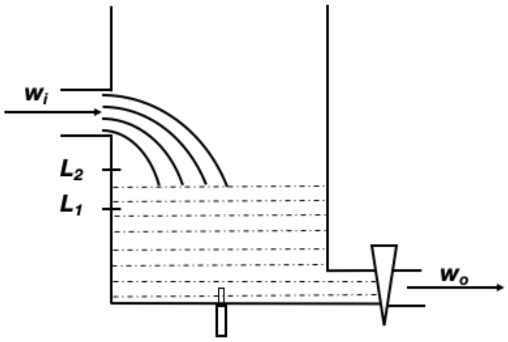


Figure 1. The Water Tank

From a logical viewpoint, the valve is connected to a Remote Terminal Unit (RTU) or Programmable Logic Controller (PLC) which interacts and communicates with the valve itself. Exchanged data is also routed to a Supervisory Control and Data Acquisition (SCADA) computer through the internal Industrial Communication Network (ICN). The SCADA system interprets and visualizes the data allowing plant personnel to monitor the position of the valve, change its position (e.g. by sending a valve position adjustment) and react to system events, i.e. troubleshooting. Other hosts are also connected to the internal ICN. As it is often the case, a demilitarized zone (DMZ) containing plant's publicly exposed services is also present. In our example, the latter are represented by a Web Server and a Mail Server. The logic schema of the previously described components is shown in *Figure 2*. The network topology is drawn by means of the CYBERWISER.eu drawing environment, where logic components are linked in a simplified way with respect to the real physical architecture. A more detailed description of the system will be discussed in Section 5.

Figure 1 shows a simplified model of the water tank consisting of the integration of three transfer functions.

- The tank transfer function, *Tank*, taking on input the current values of the incoming water flow w_i and the position *v* of the valve and sending on its output the corresponding output water flow w_o and water level *l*;
- The sensor transfer function, *Sensor*, taking on input the water level *l* and sending on its output a valve position adjustment *dv*;
- The valve transfer function, *Valve*, taking on input the adjustment *dv* and providing on its output value its new position *v*.

With respect to the case study just presented, the main risk arising due to a cyber-attack is the tank's water level either below L_1 or above L_2.

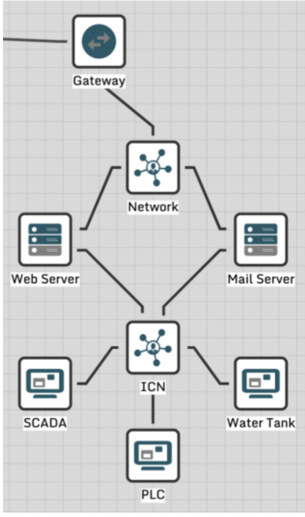


Figure 2. Water Tank physical system model.

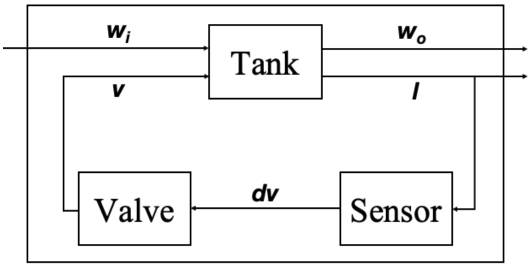


Figure 3. The Water Tank: a simplified connection.

3 Cybersecurity training challenges in industrial systems

The case study presented in Section 2 shows the paramount importance of cybersecurity training in industrial systems. However, when cybersecurity is actually seen as a requirement, a number of challenges arise:

- Training should be supplied considering the wide attack surface provided by industrial plants. Furthermore, relevant and realistic attack scenarios should be provided to trainees;
- Attack scenarios should be tailored to the specific learning goals of the trainees, rather than be general trainings;
- Training should be associated to security and unit testing of hardware and software components.

4 The CYBERWISER.eu platform

CYBERWISER.eu addresses the need for effective, user-friendly environments dedicated to training of professionals in the field of cybersecurity. It consists of an educational, collaborative, real-time civil cyber range platform currently being developed within the CYBERWISER.eu project [9]. Users can play the role of attackers (red team) and/or defenders (blue team) in different scalable and configurable scenarios. The platform is completely web-based, to facilitate adoption, collaborative support from end-users and continuous upgrade. CYBERWISER.eu expands and builds on the results and users' community of the H2020 IA named WISER [2015-2017] [10], thereby providing a jump-start situation from a consolidated raising awareness and past investment point of view. In *Figure 4* the building blocks composing the platform and their logical interplay are presented.

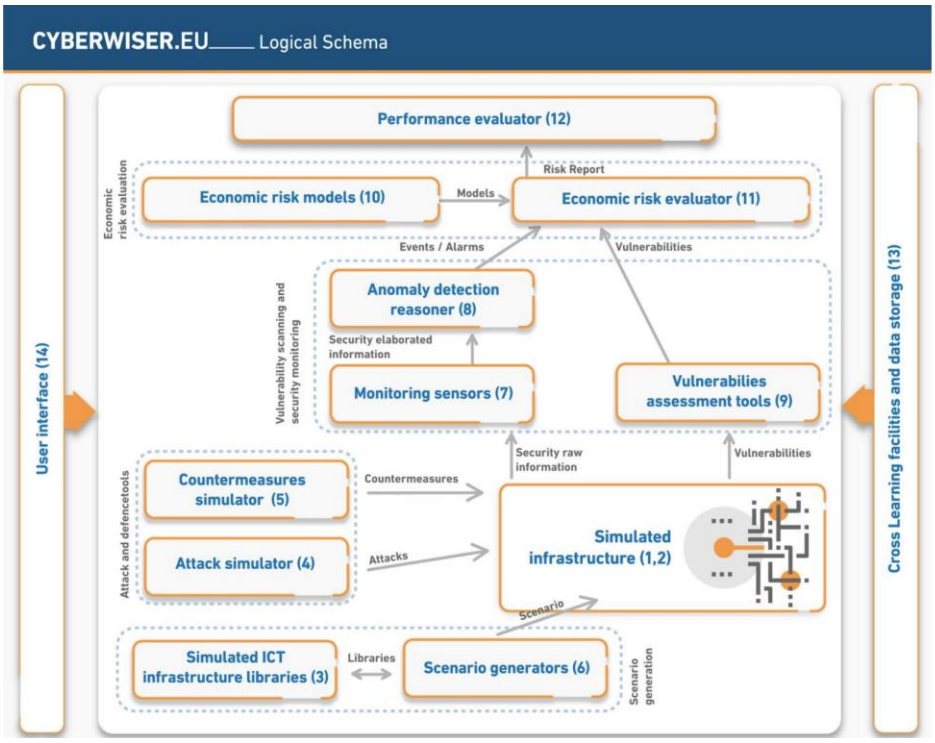

CYBERWISER.EU___ Logical Schema
Performance evaluator (12)
Risk Report
Economic risk evaluation
Economic risk models (10)
Models
Economic risk evaluator (11)
Events / Alarms
Vulnerabilities
Vulnerability scanning and security monitoring
Anomaly detection reasoner (8)
Security elaborated information
Monitoring sensors (7)
Vulnerabilies assessment tools (9)
Security raw information
Vulnerabilities
Attack and defencetools
Countermeasures simulator (5)
Countermeasures
Attack simulator (4)
Attacks
Simulated infrastructure (1,2)
Scenario
Simulated ICT infrastructure libraries (3)
Libraries
Scenario generators (6)
Scenario generation
User interface (14)
Cross Learning facilities and data storage (13)

Figure 4. CYBERWISER.eu building blocks and logical interplay among them.

CYBERWISER.eu relies on a layer of *physical machines* (1) on top of which specific *training scenarios* (2) are virtualized. To instantiate a given training scenario, there are two key elements: i) a set of *libraries* (3), containing the characterisation of a wide range of computation resources; ii) the *scenario generator* (6), which is actually in charge of the actual instantiation leveraging the libraries. To run the training sessions, the platform provides a set of tools to simulate attacks, namely the *attack simulator* (4) and also to simulate mitigation measures, namely the *countermeasures simulator* (5). The platform allows the automatic deployment of a set of *monitoring sensors* (7) playing the role of collecting relevant information with security monitoring purposes. The monitoring sensors act as collector for both performance evaluation of trainees and for sensing cyber vulnerabilities in the industrial system. The collected information is sent to the a*nomaly detection reasoner* (8), which filters and correlates information to extract relevant events. Moreover, a set of *vulnerability assessment tools* (9) are automatically deployed with the purpose of detecting vulnerabilities that may be exploited by the red team. The events and alarms generated by the anomaly detection reasoner and the vulnerabilities found by the vulnerability assessment tools are the inputs to evaluate the risk exposure related to the infrastructure. This is done by the *economic risk evaluator* (11). This element permits to quantify in economic terms how much is at risk and could be eventually lost in case of successful attacks taking place. The evaluation done by the economic risk evaluator is based on a set of innovative *economic risk models* (10) that are provided by CYBERWISER.eu. The *performance evaluator* (12) uses the economic risk calculated by the economic risk evaluator to decide, by considering a set of methodologies and guidelines defined for each specific scenario, how well the trainees are performing. The *cross-*

learning facilities (13) enriches the platform with a set of features that boosts the user experience. Finally, an integrated *graphical user interface* (14) is the interaction point with the end user.

5 Professional cybersecurity training with CYBERWISER.eu

In this section, we discuss how the CYBERWISER.eu cyber range can be exploited to address the challenges described in Section 3. Figure *5* shows the implementation of a "Water Tank" training scenario, as depicted in Section 2. The network topology comprises three different groups of scenario elements, namely *Victim*, *Attacker*, *Internet*. In this regard:

- The *Victim* group virtualizes the plant in which the water tank is placed. In particular, the water tank has been integrated by following these steps: i) modelling in *MATLAB Simulink* [15]; ii) creating a system-function (S-function) of the *Tank* Simulink block; iii) running the S-function on a virtualized machine, i.e. *Water Tank*. The *SCADA* and the *PLC* systems are also virtualized. These are connected to the Water Tank machine by means of the internal ICN. Two different servers, i.e. a web server and a mail server, are present in the DMZ.
- The *Attacker* group virtualizes the attackers' network infrastructure. In this specific scenario, the red team consists of five members. Each attacker has at disposal a virtualized *Attacker* machine running Kali Linux [11], a free Linux distribution equipped with attack and penetration testing tools.
- The *Internet* group virtualizes the Internet itself. For the sake of conciseness, all the routers in between the Attacker group and the Victim group are collapsed in one single virtualized *Core Router*. This runs the Quagga routing suite.

The scenario aims at training plant personnel, performing the role of system defenders (blue team) to protect the Water Tank machine from cyber-attacks launched by the red team. The red team is, in the meantime, performing a security test on the industrial system. This example shows also how training can be associated to security and unit testing of both hardware and software components. Indeed, it is possible to load and run vulnerability scans to check the presence of weaknesses and vulnerabilities in the industrial systems. This leads also to verifying the adoption of best practises to ensure the security of the system in a safe environment, together with research activities on the plant, before it is actually deployed. The Countermeasures simulator provides guidance in the decision-making process by suggesting a series of proposed mitigation actions based on the evolution of the attacks. Besides, a set of Vulnerability Assessment Tools with responsible for automatic assessment of vulnerabilities is given. This functionality can be used to load well-known or custom vulnerability scan in order to retrieve weakness in the industrial plant, if present. In particular, the scanning suite currently incorporates three scanning tools: i) w3af [12]; ii) OWASP ZAP [13]; iii) Nmap [14]. As an example, Figure 6 shows how a vulnerability test is applied in the SCADA machine, by means of the Vulnerability Assessment Tool. The goal of such tool is to perform a security test in software and hardware components of industrial systems.

On the opposite side, the goal of the red team is to cause the water level to fall below L_1 or exceed L_2. This happens whenever the red team can tamper the communication between the PLC and the Water Tank, or between the SCADA and the Water Tank.

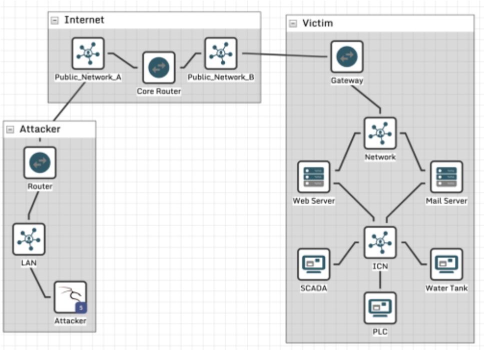
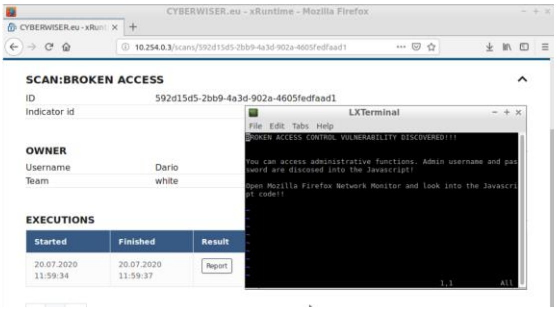


Figure 5. The Water Tank training scenario in CYBERWSIER.eu.


CYBERWISER.eu - xRuntime - Mozilla Firefox
CYBERWISER.eu - xRunt
10.254.0.3/scans/592d15d5-2bb9-4a3d-902a-4605fedfaad1
LXTerminal
File Edit Tabs Help

SCAN:BROKEN ACCESS

ID 592d15d5-2bb9-4a3d-902a-4605fedfaad1

Indicator id

OWNER

Username Dario

Team white

EXECUTIONS

Started	Finished	Result
20.07.2020 11:59:34	20.07.2020 11:59:37	Report

```
BROKEN ACCESS CONTROL VULNERABILITY DISCOVERED!!!

You can access administrative functions. Admin username and pas
sword are discosed into the Javascript!

Open Mozilla Firefox Network Monitor and look into the Javascri
pt code!!
                                                  1,1       All
```

Figure 6. Result of a security scan on the victim machine, by means of the Vulnerability Assessment Tool.

Methods generally used by adversaries to exploit SCADA systems can be found in [15]. Notice that the red team instead of a purely training purpose might have the task of testing the system behaviour under attack and unexpected input. Yet an alternative approach is to do without a red team and design a “Water Tank” training scenario whereby it is the *Attack Simulator* component that fulfils the task of performing attacks.

To conclude, it is important to highlight that during the entire duration of the training session: i) the economic risk exposure related to the infrastructure is presented to trainees by means of the *Economic Risk Evaluator*; ii) exercise progress monitoring and real-time performance assessment of the trainees is conducted by means of the *Performance Evaluator*.

6 Conclusions

In this work, we have described the main challenges related to cybersecurity training in industrial systems. The solution proposed to these challenges is an innovative cyber range platform named CYBERWISER.eu. The latter aims at providing an innovative simulated environment where realistic cybersecurity training scenarios can be designed. Scenarios give the chance to perform training exercises, simulating cyber-attacks and defence mechanism, monitoring exercises progress and real-time assessment of user performance. Additionally, the highly customizable training environments introduced the possibility to pair training with security and unit testing. The CYBERWISER.eu platform is about the democratisation of cybersecurity and the empowerment of multi-disciplined teams in public and private organisations.

7 Acknowledgements

This work has been conducted as part of the CYBERWISER.eu European project. This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 786668. This work and the content included in it do not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of its content.

8 References

[1] Cisco. Cisco 2018 Annual Cybersecurity Report (2018).

[2] ICS-CERT. Overview of cyber vulnerabilities, June 2017. https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities

[3] "2019 Cybersecurity Workforce Study - ISC2." https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study. Accessed 6 Mar. 2020.

[4] "CYBERWISER.eu" https://www.cyberwiser.eu/. Accessed 6 Mar. 2020.

[5] V. E. Urias, W. M. Stout, B. Van Leeuwen, and H. Lin, (2018). "Cyber range infrastructure limitations and needs of tomorrow: A position paper,". *In 2018 International Carnahan Conference on Security Technology (ICCST), pp. 1–5, IEEE, 2018.*

[6] Giuliano, V. and Formicola, V. (2019). "ICSrange: A Simulation-based Cyber Range Platform for Industrial Control Systems". arXiv:*1909.01910 [cs.CR].*

[7] Bliudze, S. and Krob, D. (2009). Modelling of Complex Systems: Systems as dataflow machines. *In 2009 Fundamenta Informaticae, vol. 91 (2), pages 251-274.*

[8] Bernardeschi, C. and Domenici, A. (2016). "Verifying safety properties of a nonlinear control by interactive theorem proving with Prototype Verification System". *In 2016 Information Processing Letters, vol. 116, Issue 6, Pages 409-415.*

[9] "CYBERWISER.EU Project | H2020 - Cordis." 6 Sep. 2019, https://cordis.europa.eu/project/id/786668. Accessed 6 Mar. 2020.

[10] "WISER Project | H2020 - Cordis." 24 Jul. 2017, https://cordis.europa.eu/project/id/653321. Accessed 6 Mar. 2020.

[11] Kali Linux Distribution. https://www.kali.org

[12] w3af. http://w3af.org/

[13] OWASP ZAP. https://owasp.org/www-project-zap/

[14] Nmap. https://nmap.org/

[15] "Simulink - MathWorks." https://it.mathworks.com/products/simulink.html. Accessed 6 Mar. 2020.

[16] Bartman, T. and Carson, K. (2016). "Securing communications for SCADA and critical industrial systems". *In 2016 69th Annual Conference for Protecting Relay Engineers (CPRE).*

[17] Hallaq, B., Nicholson, A., Smith, R., Maglaras, L., Janicke, H., & Jones, K. (2018). "CYRAN: a hybrid cyber range for testing security on ICS/SCADA systems". In Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications (pp. 622-637). IGI Global.

[18] Darwish, O., Stone, C. M., Karajeh, O., & Alsinglawi, B. (2020, April). Survey of Educational Cyber Ranges. In Workshops of the International Conference on Advanced Information Networking and Applications (pp. 1037-1045). Springer, Cham.

[19] Yamin, M. M., Katt, B., & Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security, 88, 101636.