EVA: a hybrid cyber range

EVA: A Hybrid Cyber Range*

Shabeer Ahmad[13], Nicolò Maunero[23], and Paolo Prinetto[23]

[1] GSSI - Gran Sasso Science Institute, L'Aquila, Italy
shabeer.ahmad@gssi.it
[2] Politecnico di Torino, Dipartimento di Automatica e Informatica, Torino, Italy
nicolo.maunero@polito.it
paolo.prinetto@polito.it
[3] CINI - Cybersecurity National Lab

Abstract

Over the recent years, cyber attacks have increased constantly. Attacks targeting sensors networks, or exploiting the growing number of networked devices, are becoming even more frequent. This has led to the need to find a way to train the teams responsible for defending computer systems in order to make them able to respond to any threats quickly. The fact that it is impossible to carry out training operations directly on corporate networks or critical infrastructure has led to the birth of Cyber Ranges, virtual or hybrid systems that allow training in safe and isolated environments. In this paper we present a model for the implementation of a Hybrid Cyber-Range (HCR), based on the model of a real Water Supply System WSS). The HCR shall combine the dynamism and flexibility of virtualised Cyber-Ranges (CR) and the realism of Cyber-Physical Systems (CPS).

1 Introduction

The unification of physical systems and networked computing opened a new era of specialised systems, usually referred to as *Cyber-Physical Systems* (CPS) The term "cyber-physical systems" appeared in 2006 and become popular in 2010, first used by Helen Gill at the National Science Foundation in the US to mention the combination of cyber computation with physical processes [11]. A CPS is a high-scale network system consisting of sensors, actuators, control processing units, and communication devices [5]. Over the recent years, CPSs have received increasing attention due to their intrinsic combination of physical and cyber aspects, in particular, regarding the aspect of cybersecurity [10, 4].

Industrial control systems (ICS) are a sub-class of CPSs where control processes and physical actions are under-control of cyber components (PLCs, SCADA, etc.). Any cyber-attacks on ICS or critical infrastructures such as water supply system, transportation, power grid and so on[1], may lead to series of serious problems and the consequences for people and infrastructures can be disastrous.

The concern about cybersecurity of critical infrastructure, in recent years, stimulated the creation and adoption of new methodologies for the training of cybersecurity teams in charge of defend them. This lead to the introduction of the concept of *Cyber Range* (CR). Cyber Ranges are virtual polygons dedicated to the training of cybersecurity professionals, consisting of controlled and safe environments, typically based on virtualisation [3].

It is shown in literature that malicious attackers use realistic testbeds to develop complex exploits, such as, Advanced Persistent Threats (APTs) [12]. This therefore requires the use of

[1] https://www.cbsnews.com/news/cyber-war-sabotaging-the-system-06-11-2009/

a type of CR that integrates, within it, also real components used in ICS and critical infrastructures, to increase its realism [23]. Hereinafter, we will identify this type of CRs as *Hybrid Cyber Ranges* (HCRs).
In this paper we present EVA, an Hybrid Cyber Range based on the model of a Water Supply System. The objective of EVA is to provide a realistic testbed, representing in the best way, and as faithfully as possible, a real Water Supply System. Moreover it shall also provides the flexibility of a CR in deploying different scenarios and the possibility to easily test new products and/or solutions before adopting them in a real system. The paper is structured as follows: first a brief overview on CRs developed by both industry and academy and the definition of the various teams that interact with a CR. Then the model and implementation of EVA, the emulator of a real aqueduct, is presented, continuing with the introduction of the model adopted for upgrading EVA from a CPS to a HCR. Some improvements and issues to be addressed in the near future are eventually presented.

2 Background

2.1 Cyber Range

A Cyber Range (CR) is a platform that can provide advanced cyber-security training exercises for university students and professionals, changing the way to approach cybersecurity[2]. In as document of 2018 [16] NIST defines a Cyber Range as "*an interactive, simulated representation of an organisation's local network, system, tools, and applications that are connected to a simulated internet level environment.*"
The use of CRs derives from the need to have protected and secure environments where performing cybersecurity activities, isolated from the outside world and without the need to operate directly on the corporate networks or infrastructures under analysis.
Three different types of CR can be identified:

Physical Cyber Ranges : the testbed faithfully recreates a network or computing infrastructure, guaranteeing the highest level of loyalty, often using real components of the reference infrastructure. This typology is, on the one hand, the best for gaining experience and gathering results with the aim of improving the defences of a given infrastructure. On the other hand, it has the disadvantages of (i) being less flexible, since a modification may require the reconstruction of the entire CR, and (ii) requiring a very expensive set-up process.

Virtual Cyber Ranges : in the testbed all the components of the reference infrastructure are simulated, using virtualisation technologies, to obtain testbeds of different complexity. The main advantage of this approach is that the components needed to build it (servers for hosting virtual machines) can be easily found, at a relatively low cost, on the market. It is also possible, in this case, to get a high degree of flexibility and scalability in changing the simulated environment. However, this approach has the disadvantage of not providing an experience very similar to the real one.

Hybrid Cyber Ranges : sometimes referred as *Cyber-Physical Ranges*, this typology is a hybrid of the two previous ones. It aims to combine the positive aspects of both approaches, having the flexibility of a virtual environment with the realism resulting from the use of real-word hardware components of the reference infrastructure.

[2] https://www.merit.edu/cyberrange/

2.2 Teams Definition

One of the most eminent and successful training activities that a Cyber-Range could offer is the one in which it provides a battlefield where different teams oppose each other [13].

Red Teams are normally composed of a small number of experts who have the task of attacking or compromising the security simulated scenario, organization or infrastructure. They must be well conscious of the so-called TTP (Tactics, Techniques and Procedures) of the attackers [19].

Blue Teams have the task of defending the scenario and have the mentality of the defenders and are trained to detect, respond, and mitigate the attacks done by Red Teams. Members of the Blue Team need to stop unauthorised or illegal activities by mitigating potential vulnerabilities. The capabilities and expertises of Blue Team's strongly effect the whole exercise scenario [17].

White Team responsible for the design and construction of the scenario used for the exercises. Moreover, the White Team acts as supervisor on exercises involving attack and defence paradigm, establishing the final score. It is essential for the White Team to make sure that the exercise is conducted according to the scenario and according to the objective.

Admin Team the administration team is responsible for the supervision of the entire cyber range, are in charge of monitoring the session and assigning scores to each team.

Design Team is composed of the persons in charge of the design of the reference infrastructure on which the CR is based.

2.3 State-of-the-Art

2.3.1 Physical CRs

As far as Physical Cyber Ranges are concerned, it is very difficult to find examples in literature of testbed with high level of fidelity with respect to the real-word target infrastructure, both because of the difficulty of implementing this type of CRs and because the construction of such structures would often require the disclosure of business secrets and/or the precise topology of the internal network.

The most prominent and ambitious project of physical cyber range is Cybertropolis [8], a project of the United State (U.S.) Department of Defence (DoD), situated at the Muscatatuck Urban Training Complex (MUTC)[3]. In continuous evolution and improvement, it aims to provide participants with the opportunity to interact with a real-word scenario. In fact, it allows the integration of different dimensions, such as role-players, and interaction with a hyper-realistic environment. It is composed of several elements such as a prison complex, a full size functioning water treatment plant and waste water treatment plant, a state-of-the-art implementation of internet of things systems for smart homes, and so on.

Ahmed et al. proposed a SCADA system testbed [1] for research and training. Built using real-world industrial components, it its composed of models of a waste water treatment plant, a power transmission and distribution systems and a gas pipeline. All these systems are small-scaled but fully functionals. The main drawback of this project is that it provide insufficient scalability and flexibility and does not give the possibility to design different attack scenario.

[3] https://www.atterburymuscatatuck.in.ng.mil/Muscatatuck/CyberTropolis/

Aditya et al. proposed SWaT [14], a testbed based on a model of a Water Supply System. Also in this case is a small-scale, fully functional model built with real-world industrial components. The goal of the project is to have a safe testbed where to research possible vulnerabilities and test new cyber defence strategies. As before, the main drawback of this project is that it provide insufficient scalability and flexibility as well as the impossibility to deliver different attack scenario for cyber defence training.

2.3.2 Virtual CRs

Virtual Cyber Ranges are the most common and used thanks to their flexibility and relatively low building and maintenance costs. KYPO Cyber Range is a Czech project [24] funded by the Ministry of the Interior of the Czech Republic as part of the Security Research Program of the Czech Republic. The Objectives of the KYPO Project was to build a scenario for carrying out research and developing methods for mitigating attacks on critical infrastructure in the Czech Republic.

The Michigan Cyber-Range[4] is powered by Merit Network Network[5], the nation's longest-running research and education network. Above all, Michigan Cyber Range is the largest unclassified network, especially designed for cybersecurity training and It offers courses including Penetration Testing, Ethical Hacking, Vulnerability Assessment, Secure Coding, and Digital and Networking Forensics.

Emulab and DETER are two of the most renowned emulation facilities for Virtual Cyber Ranges developed in academia for performing cyber-security training and exercises. Emulab [21], was launched by University of Utah and was used for both university facilities and open source emulation software for testbeds. The Emulab software is used in more than twenty other emulation testbeds over the globe and it is mainly utilised for carrying out research in the fields of networking and distributed systems. DETER[6] (a derivative of Emulab), founded by the Department of Homeland Security and the Department of Defence, is an emulation-based cyber-range having more capabilities as compared to Emulab. The DETER testbed is used for medium size national-level experimentation and training in cybersecurity.

DARPA (Defence Advanced Research Project Agency) commenced the (U.S.) National Cyber-Range (NCR) plan to design the architecture and software tools required for a secure, self-contained cyber testing amenity [18]. DARPA (NCR) is probably the most famous and ambitious project for cyber-defense training with the aim of simulating cyber-attacks on computer networks, it is planned to be built on a large scale to emulate the complexity of commercial networks and it should allow new cyber technologies to be tested and validated in a representative environment.

The Cisco Cyber Range [7] offers a specialised technical training activity to assist staff responsible for the security to create and improve the skills and experience needed to answer modern cyber-threats. CISCO Cyber Range offers a specialises scenario that enables security-staff to play the role of both attacker and defender to discover the latest techniques of vulnerability exploitation and utilizing advanced tools tactics and techniques to minimise and remove threats.

[4] https://www.merit.edu/cyberrange/
[5] https://www.merit.edu
[6] https://deter-project.org

2.3.3 Hybrid CRs

The Hybrid Cyber Range, as mentioned above, aims to combine the versatility of virtualisation with the realism of real components of the infrastructure that has to be recreated. There are several projects in this field, both academic and industrial, usually focused on critical infrastructures such as Water Supply Systems and Power Plants [6, 9].

In 2016 Ashok et al. proposed a testbed for assessing security of Smart Grid called PowerCyber [2]. It's a project of the Iowa State University, composed of a mix of real hardware, software emulated components and virtualization technologies for scalability. It is remotely accessible and can be used for simulating different cyber attack scenarios.

Tebekaemi et al. proposed an hybrid testbed [22] for assessing the security in communication protocols in smart grid. This testbed is composed of a combination of real hardware components and virtualized ones. This approach allows for a great scalability and modularity since new components can be added easily and the virtualisation of some components helps in keeping the overall cost small. However this system is built with the specific goal of security assessing and thus it does not implement any functionalities allowing different attack scenarios for training purposes.

3 Our Goal

Our goal is to implement a Hybrid Cyber Range (HCR) through which we can, on the one hand, assess the security of a CPS and, on the other hand, make serious gaming events and/or training teams while combining the flexibility of a CR and the realism of a CPS.

As a first step, EVA, an emulator of a real Water Supply System, was built. It is a fully functional small scale model of a WSS composed of industrial components and devices to achieve the maximum realism (see Section 4). Then was necessary to equip EVA with additional feature to make it able to serve also as a Cyber Range (CR). The HCR based on EVA must have some specific features and need to be used in different context:

- **Training the Blue Teams**: Blue Teams need isolated and secure environments where they can be trained. It is often unfeasible to use the real network or infrastructure for training activities. But the team responsible for defending the corporate infrastructure or network must be able to respond to real threats quickly. For this reason our HCR must have the necessary flexibility to support the development of different attack scenarios while maintaining a good realism to have an experience of use and interaction as close as possible to the real one.

- **Training the Design Team**: the Design Team can take advantage of the use of an HCR as this would give them the flexibility to test new solutions before using them in the field, having an isolated environment, but at the same time realistic and very similar to the real one.

- **Mock up**: for our purposes it is necessary that the HCR is responsible for an easy and fast replacement and/or addition of new components and devices. This is because many companies, especially those operating in the field of critical infrastructure, need a system with which to test new components before using them in the field.

See Section 5 for more detail about EVA as a HCR.

4 EVA as a CPS

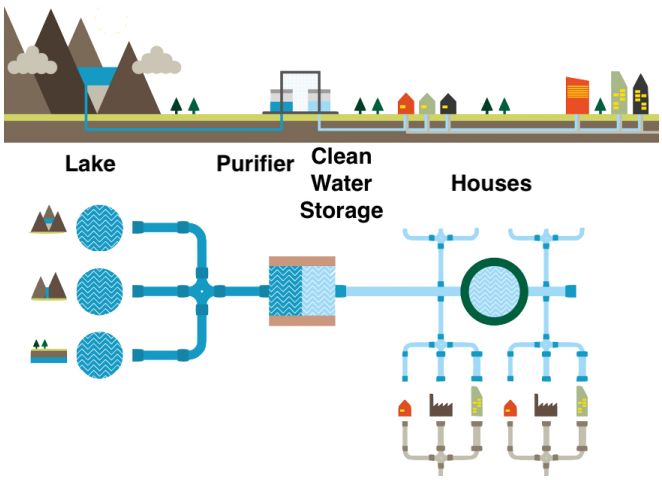

Figure 1: Architecture of the real Water-Supply System

EVA (Emulatore di Vero Acquedotto - Emulator of a Real Aqueduct) is a CPS representing a functioning model of a real Water Supply System (WSS). Apart from the basic components such as tanks, pipes, pumps etc., EVA comprises sensors, actuators, communication protocol, and SCADA/ICS as a controller. The IT and OT part of EVA are composed of industrial components used in the real WSS, including the SCADA, but other component, such as pump and sensors, are low-quality equipment just used in this first phase of building the model. The physical system was designed according to the architecture of a real WSS shown in Figure 1[7]. As a general overview, the model works in the following way. The water is gathered from a source, that can represent a lake or aquifer. The water is then purified and collected in a dedicated storage system before being distributed to the customers (people houses, hospital or other infrastructures).

4.1 EVA Implementation

Figure 2 sows the model design and the interconnection between all the components of EVA. The system configuration is based on a star topology, with a single master in the center and multiple slaves on the vertexes. The different Raspberry Pis[8] functioning as slaves are connected on the same local network using WiFi with Internet access. The role of the master is played by the JACE 8000[9] controller. Using this component it is possible to implement a Web Application with the same functionality of a SCADA, but with all the advantages that its virtualisation can bring. The user, according to his privileges, can remotely supervise the entire structure: data logging, alarms, network management and maintenance of the control logic of the entire plant. The master and the slaves share commands and data using the Modbus protocol[10]. This

[7] Image taken from https://cargocollective.com/crockhaus/filter/aqueduct--water-system-acquedotto-infographic-infografica-filera-water-acqua-italia-crockhaus-matteo-riva-illustration-how-it-works-vita-non-profit-magazine

[8] https://www.raspberrypi.org/

[9] https://www.tridium.com/products-services/niagara4

[10] http://www.modbus.org/

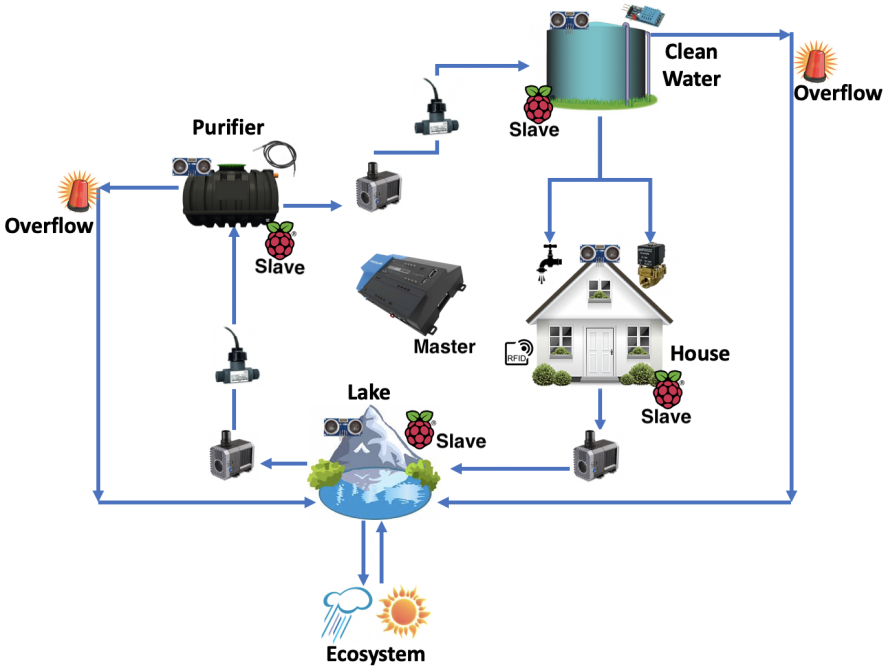

Figure 2: EVA Implementation Schema.

protocol has been chosen because is one of the most used in industrial facilities. The slaves Raspberry Pis are directly connected to sensors and actuators. In a first phase data are collected and sent to the controller, in charge of analysing informations and decide whether or not to activate actuators and, thus, sending the appropriate commands to the slaves. Since sensor and actuators are low quality components the purpose of the Raspberry Pi slaves is to implement the communication protocol, Modbus, for communicating with the master controller. Finally, also the external environment, namely ecosystem, was implemented in order to give a more realistic view of the system.

5 EVA as a Cyber Range

In order to convert EVA into a Cyber Range, we must first provide a way to quickly and easily change the behaviour of the system for representing different scenarios. In addition we should avoid changing a large part of the composition of the system to represent different scenarios, since this would require high maintenance costs.

5.1 Model

EVA, as any other CPS, can be modelled splitting its architecture in term of several *components*, being them hardware or software; a possible model is shown in Figure 2, where components are exchanging information items (data, states, and controls) via proper physical communication infrastructures, wired or wireless, indifferently. In order to upgrade EVA to serve as a Cyber Range, a plenty of "flexibility" has to be introduced in its structure, to allow all the involved

CR teams, 2, to properly work at their best. From both a conceptual and a practical point of view, the structure of Figure 2 has to be modified, inserting an additional *Wrapper* on top of each components, aimed at providing the possibility of dynamically changing the behaviour of the underlying component without physically modifying it. More details in the next section 5.2. In few words, through the use of the *Wrapper* it is possible to change the input and output of the given component, changing the source of these signal accordingly to the requirements of the scenario.

5.2 Wrapper

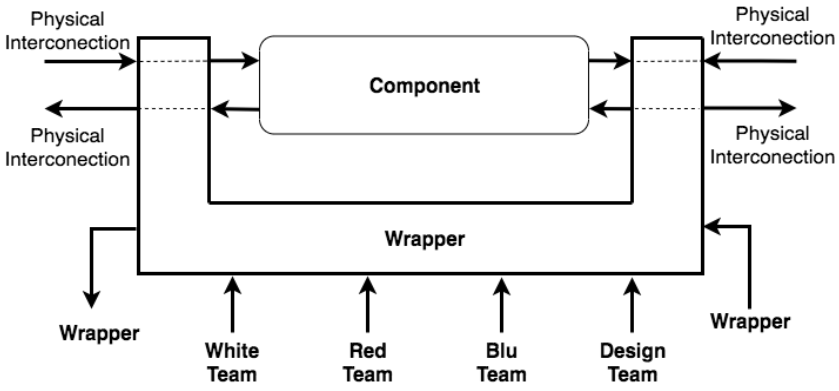

Figure 3: Wrapper.

In the previous section the concept of *Wrapper* has been introduced. Within the CR model this new component will give the possibility to get the flexibility required to serve different purposes, being them training, gaming or mock-up. As you can see in Figure 3, the *Wrapper* connects directly to all the inputs and outputs of each component of the CPS. It will therefore be possible to arbitrarily control the inputs and outputs of the component by choosing the appropriate source based on the scenario. In terms of model, the *Wrapper* is composed by:

- *Wrapper Controlloer*: this allows to control the behaviour of the *Wrapper* modifying the interconnection and data exchange inside it;
- *Wrapper Data & Interconnection*: managed by the *Wrapper* Controlle defines how inputs and outputs of the component are routed.

Moreover *Wrappers* can communicate directly between each other by means of a dedicated interconnection, bypassing components or physical interconnections, this for allowing a greater flexibility in the scenario definition and implementation. In general the *Wrapper* can work in the following ways:

- **Normal Mode**: the *Wrapper* does not interact with the component, not changing the component inputs and outputs in any way. This mode of operation can be used when it is necessary to study the properties of the CPS in general or the specific component in particular to discover potential vulnerabilities.
- **Vulnerability Injection**: the *Wrapper* takes control of the inputs and outputs of the component for inserting a vulnerability not previously present. This mode of operation

is used by the White Team during the design and deployment of the scenario, this could mean, in practice, for example changing the software running on a specific component.

- **Vulnerability Remediation**: the *Wrapper* take control only of the component inputs. In this mode of operation those who interact with the *Wrapper*, the Blu Team, should not notice its presence. The Blu Team will interact with the component, as it would do in a normal way, to be able to apply patches to vulnerabilities (perhaps introduced previously by the White Team).

- **Attack Injection**: the *Wrapper* takes control of the component's inputs and outputs. The Red Team can use this mode to carry out a campaign of attacks. It is particularly useful in the training phase of the Blu Team as it allows the Red Team to simulate an attack even in the absence of a specific vulnerability (think of the case of a sensor/actuator, the insertion of a vulnerability would require replacement of it). By modifying the component inputs, the Red Team will be able to simulate a direct attack on that component, while, by modifying the outputs appropriately, it will be able to simulate an attack starting from that component.

- **Behaviour Modification**: the *Wrapper* takes control over the inputs and outputs of the connected component. The Design Team can take advantage of this mode to emulate new components or interconnections and protocols, bypassing the existing ones, thanks also to the direct interconnection between two *Wrapper*. It is therefore possible to test new solutions, both hardware and software, without the need to modify or rebuild the cyber physical model.

- **Mock Up**: the flexibility introduced by the use of *Wrappers* around each component can become useful also for mock-up operations. New components, being them hardware or software, can be easily added to the CPS without the need of rebuilding the entire system from scratch, while maintaining a good enough realism to gather information about the performance of the new components before adopting them in the real system.

6 Attacks Modelization

Given the model proposed in the section 6.1 and the cyber physical model on which the proposed CR is based, we can now see some examples of attacks on similar systems and how these can be easily modelled with the proposed CR.

6.1 False Data Injection Attacks

As reported in [15] these attacks can be divided into Response Injection Attacks and Command Injection Attacks, both possible because network of ICS often do not use authentication for packets. As far as response injection attacks are concerned, the objective is to intercept, modify and forward the packets containing the measurements coming from the sensors. Allowing, for example, to switch off pumps of an aqueduct by making the central control system believe that critical limits have been reached. Command injection attacks instead, works in a similar way but, an attacker intercepts the commands sent by the central control system to the actuators. He then proceeds to modify them appropriately and then forwards the desired commands. In the specific case of EVA it is possible to easily model and simulate this attack thanks to the use of the *Wrapper*. In a training scenario, the Red Team responsible for the attack campaign,

in one case, will take control over the outputs of the sensor (Figure 4), sending arbitrary data to the central control unity, bypassing the actual sensor outputs.
In the second case, instead, the *Red Team* will take control over the actuator inputs (Figure 4) sending, then, arbitrary command bypassing the ones coming from the central control unit.

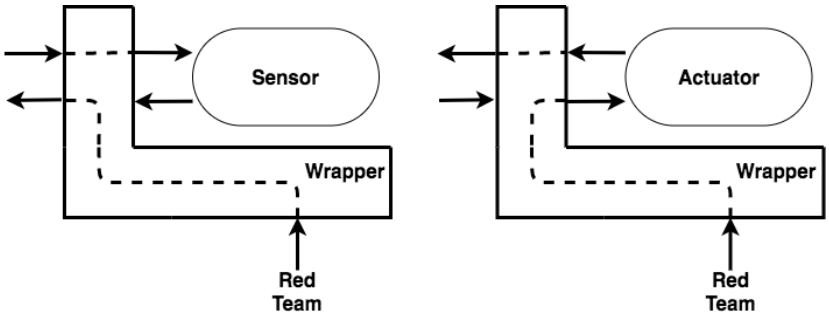

Figure 4: Attack Emulation Using the *Wrapper*.

7 Open Issues & Future Works

In Section 5 the model for the Hybrid Cyber Range EVA has been presented. The work is still in development but it is possibile to identify which are the key issues to address during the project development.
The CINI Cybersecurity National Laboratory[11] has started CyberRange.IT: a national project for creating a platform for the development of the future Italian cybersecurity community. This platform is a network of nodes distributed throughout the national territory and each specialized on different vertical domains. Each node must offer its users the facilities for learning, carrying out research, and practical training with cyber threats and challenges originated from the real world. EVA, within this project, must provide a testbed representing a Water Supply Systems.
Is therefore crucial that the HCR can be remotely accessible and can provide all the functionalities to be interconnected with other CR to create a network of distributed testbed. Another important aspect to be considered is the integration of an orchestrator, to manage the *Wrapper* functionalities, for scenario deployment. In this case, as shown in [20], can be used TOSCA [12] a orchestrator language released under Oasis Open Standard.

8 Conclusions

In this paper we have presented a model of Hybrid Cyber Range with the aim of obtaining a system that is flexible in its use but realistic. The model presented is valid for any CPS that wants to be transformed into HCR. In this specific case, the modeling was based on EVA, a model of WSS.
Thanks to the introduction of a *Wrapper* for each component it has been possible to expand the functionality of EVA, while avoiding re-building the system, making it possible to deploy different scenarios for competitions or training.

[11] https://www.consorzio-cini.it/index.php/it/lab-nazionali/lab-cyber-security-2
[12] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=tosca

References

[1] Irfan Ahmed, Vassil Roussev, William Johnson, Saranyan Senthivel, and Sneha Sudhakaran. A scada system testbed for cybersecurity and forensic research and pedagogy. In *Proceedings of the 2nd Annual Industrial Control System Security Workshop*, pages 1–9. ACM, 2016.

[2] A. Ashok, S. Krishnaswamy, and M. Govindarasu. Powercyber: A remotely accessible testbed for cyber physical security of the smart grid. In *2016 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, pages 1–5, Sep. 2016.

[3] R. Baldoni and R. De Nicola. The future of cybersecurity in italy. *CINI-Consorzio Interuniversitario Nazionale Informatica*, 2016.

[4] Martín Barrère, Chris Hankin, Angelo Barboni, Giulio Zizzo, Francesca Boem, Sergio Maffeis, and Thomas Parisini. Cps-mt: A real-time cyber-physical system monitoring tool for security research. In *2018 IEEE 24th International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA)*, pages 240–241. IEEE, 2018.

[5] Alvaro A Cardenas, Saurabh Amin, and Shankar Sastry. Secure control: Towards survivable cyber-physical systems. In *2008 The 28th International Conference on Distributed Computing Systems Workshops*, pages 495–500. IEEE, 2008.

[6] Mehmet Hazar Cintuglu, Osama A Mohammed, Kemal Akkaya, and A Selcuk Uluagac. A survey on smart grid cyber-physical system testbeds. *IEEE Communications Surveys & Tutorials*, 19(1):446–464, 2016.

[7] CISCO. Cisco cyber range. https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/asf-cyber-range-large.pdf, 2016. [Online; accessed 28-November-2019].

[8] Gary M Deckard. Cybertropolis: breaking the paradigm of cyber-ranges and testbeds. In *2018 IEEE International Symposium on Technologies for Homeland Security (HST)*, pages 1–4. IEEE, 2018.

[9] Hannes Holm, Martin Karresand, Arne Vidström, and Erik Westring. A survey of industrial control system testbeds. In *Nordic Conference on Secure IT Systems*, pages 11–26. Springer, 2015.

[10] Abdulmalik Humayed, Jingqiang Lin, Fengjun Li, and Bo Luo. Cyber-physical systems securitya survey. *IEEE Internet of Things Journal*, 4(6):1802–1831, 2017.

[11] Frank Jiang and Michael R Frater. Towards a reliable aquatic-based cyber physical system: A new contextsituation aware low overhead routing scheme. In *2013 IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems*, pages 30–35. IEEE, 2013.

[12] KasperskyLab. Threat landscape for industrial automation systems. https://ics-cert.kaspersky.com/reports/2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018/, 2019. [Online; accessed 28-November-2019].

[13] Hannes Krause. Nato on its way towards a comfort zone in cyber defence. *The Tallinn Papers*, 1(3):1–6, 2014.

[14] Aditya P Mathur and Nils Ole Tippenhauer. Swat: a water treatment testbed for research and training on ics security. In *2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater)*, pages 31–36. IEEE, 2016.

[15] Thomas H Morris and Wei Gao. Industrial control system cyber attacks. In *Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research*, pages 22–29, 2013.

[16] NIST. Cyber ranges. https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf, 2018. [Online; accessed 28-November-2019].

[17] Victor-Valeriu Patriciu and Adrian Constantin Furtuna. Guide for designing cyber security exercises. In *Proceedings of the 8th WSEAS International Conference on E-Activities and information security and privacy*, pages 172–177. World Scientific and Engineering Academy and Society (WSEAS), 2009.

[18] Michael Rosenstein and Frank Corvese. A secure architecture for the range-level command and

control system of a national cyber range testbed. In *CSET*, 2012.

[19] Robin Ruefle, Audrey Dorofee, David Mundie, Allen D Householder, Michael Murray, and Samuel J Perl. Computer security incident response team development and evolution. *IEEE Security & Privacy*, 12(5):16–26, 2014.

[20] Enrico Russo, Gabriele Costa, and Alessandro Armando. Scenario design and validation for next generation cyber ranges. In *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*, pages 1–4. IEEE, 2018.

[21] Christos Siaterlis, Andres Perez Garcia, and Béla Genge. On the use of emulab testbeds for scientifically rigorous experiments. *IEEE Communications Surveys & Tutorials*, 15(2):929–942, 2012.

[22] Eniye Tebekaemi and Duminda Wijesekera. Designing an iec 61850 based power distribution substation simulation/emulation testbed for cyber-physical security studies. In *Proceedings of the First International Conference on Cyber-Technologies and Cyber-Systems*, pages 41–49, 2016.

[23] Vincent E Urias, William MS Stout, Brian Van Leeuwen, and Han Lin. Cyber range infrastructure limitations and needs of tomorrow: A position paper. In *2018 International Carnahan Conference on Security Technology (ICCST)*, pages 1–5. IEEE, 2018.

[24] Jan Vykopal, Radek Ošlejšek, Pavel Čeleda, Martin Vizvary, and Daniel Tovarňák. Kypo cyber range: Design and use cases. 2017.