CONCEPTUAL SOLUTION OF THE TRAINING KITS FOR CRITICAL INFRASTRUCTURE CYBER SECURITY – CASE STUDY: OPEN-LOOP PUMPED STORAGE HYDROPOWER

Vule Reljić [1] [ORCID 0000-0001-6496-5651], *Dragan Šešlija* [1] [ORCID 0000-0002-2133-008X], *Vladimir Jurošević* [1] [ORCID 0000-0001-9913-2473], *Valentina Mladenović* [2] [ORCID 0000-0001-6642-340X]

[1] *Faculty of Technical Sciences, Department of Industrial Engineering and Management,Novi Sad*

[2] *Technical College of Applied Sciences at Zrenjanin, Department of Mechanical Engineering, Electrical Engineering and Computer Science, Zrenjanin*

Abstract: *Critical infrastructure (facilities, systems, networks etc.) is of key significance for any country and their security is of utmost importance. As computer networks are integral parts of critical infrastructure (CI) and highly vulnerable to malicious attacks, a special attention must be paid on cyber security (CS). Therefore, in this paper, the basis as well as key requirements for the development of training kits for testing the CS of CI are presented on the example of open-loop pumped storage hydropower (PSH). The training kits should be easily portable and easy to install and demonstrate.*

Key words: critical infrastructure, training kit, open-loop pumped storage hydropower

1. INTRODUCTION

The state, as an organization, is obliged to defend national security, i.e. protect its citizens, economy, and institutions. Historically, national security primarily focused on safeguarding against military threats. However, modern national security now encompasses protection against terrorism, crime, economic risks, energy vulnerabilities, environmental challenges, food safety, information breaches, and CI protection (Viganò et al., 2020).

As per the Law on CI of the Republic of Serbia (Službeni glasnik RS, 87/2018), CI refers to systems, networks, facilities, or their components. The disruption of their functioning or the supply of goods and services can have severe consequences for national security, public health and safety, property, the environment, citizen well-being, economic stability, and the functioning of the Republic of Serbia. The law identifies eight sectors as CI: energy, transport, water and food supply, health, finance, telecommunications and information technologies, environmental protection, and government operations.

Power system disruptions pose significant risks to national security and the economy (Ten et al., 2010). Today, power systems rely on complex Internet of Things (IoT) and Supervisory control and data acquisition systems (SCADA) vulnerable to various attacks (Maglaras et al., 2018), necessitating special attention in this sector. However, due to the complexity and interdependence of the telecommunications and information technologies sector, achieving the required level of security is challenging.

Numerous training programs and courses have been developed to address the CS of CI (Chowdhury & Gkioulos, 2021). Research has shown that the outcome of attacks on CI often depends on the lack of awareness and practical training among personnel (Ghafir et al., 2016). Adequate personnel training is crucial for achieving the necessary security level in CI.

This paper presents the conceptual solution of training kits used for examining and testing the CS of CI, using an open-loop PSH as an example. The paper is organized as follows: Section 2 presents the requirements for the desing of traing kits, while Section 3 briefly outlines the types and structure of PSH as well as different operating scenarios of the open-loop PSH. Based on these scenarios, Section 4 provides a proposal for the structure of the training kit, and Section 5 highlights the most important conclusions of the study.

2. REQUIREMENTS FOR THE DESIGN OF TRAINING KITS FOR CS OF CI

In order to increase the CS of CI it is necessary to develop a new kind of training kits which will facilitate presentation of the functionality of CS software. There are several key requirements:

- Training kit should adequately represent the functionality of the chosen CI. This implies the real motion of critical elements of infrastructure (flowing of water in PSH, moving of nuclear rods in nuclear power plants etc.).
- Training kit should comprehend all the necessary computer-controlled hardware (pumps, directional control valves, motors, actuators, sensors, etc.) as well as software (software for Programmable Logic Controller (PLC), Human Machine Interface (HMI), communication software etc.).
- Design of training kit should take into consideration the potential for various attacks to CI.
- Training kit should be portable. This implies that it should be embedded in no more than two suitcases. Also, suitcases should not be too heavy in order that one man can handle them.
- Training kit should be assembled on site in a relatively easy manner.
- Training kit should be able to stand freely on the table in order to be easily viewed.

According to these requirements a conceptual solution of a training kit for open-PSH is shown.

3. CASE STUDY: PUMPED STORAGE HYDROPOWER

This paper focuses on developing a training kit to examine and test the CS of the open-loop PSH. Hydropower plants produce electricity using kinetic energy of water, driving turbines connected to electricity generators. There are three types of hydropower facilities: impoundment, diversion, and pumped storage. PSH, with upper and lower water reservoirs, can be open-loop or closed-loop pumped storage systems, as shown in Figure 1.

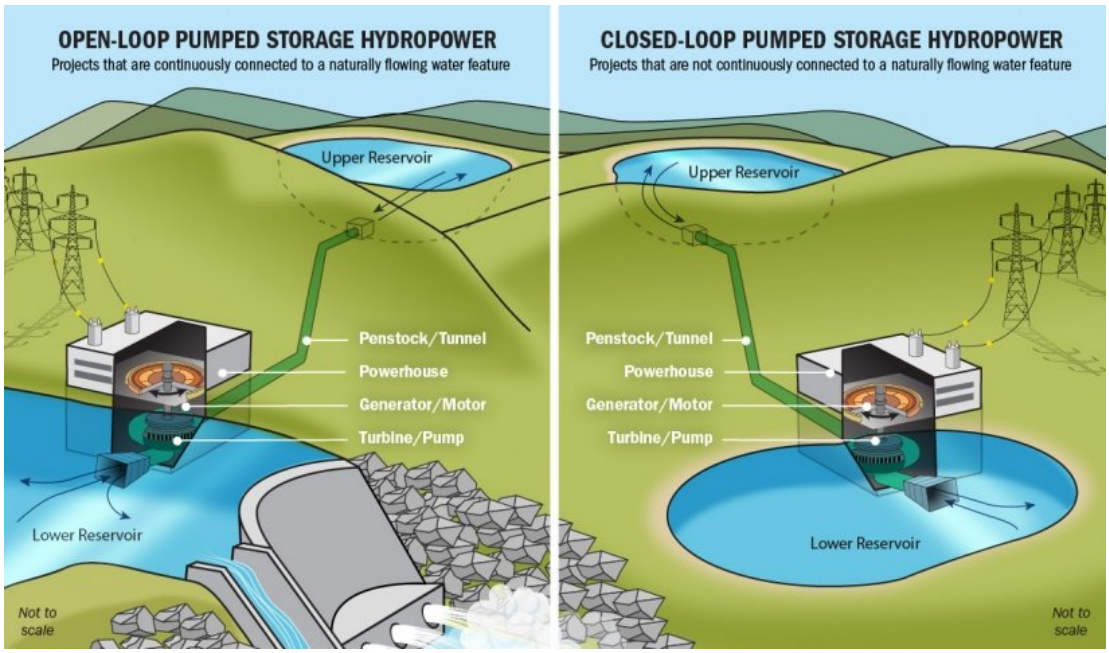

Figure 1: Different configuration of PSH (U. S. Department of Energy, 2023)

The first known use cases of PSH were found in Italy and Switzerland in the 1890s (*U. S. Department of Energy, 2023*). Now, PSH facilities can be found all around the world. In the Republic of Serbia, there is one open-loop PSH named "Bajina Bašta" (Figure 2). This PSH features an upper reservoir in the Beli Rzav river valley and a lower reservoir connected to the existing "Bajina Bašta" hydropower on the Drina river (Elektroprivreda Srbije, 2023-2).

Figure 2: PSH "Bajina Bašta" (Elektroprivreda Srbije, 2023-1)

3.1 Operating scenarios

Four distinct operational scenarios of a PSH can be defined based on the natural cycle of water circulation. These scenarios, suitable for simulation using a training kit, include:

- Normal operation mode;
- Reversible operation mode;
- Emptying the upper reservoir;
- Filling and emptying of the lower course of the river.

During the normal operation mode operation, water flows into the main, lower reservoir, and subsequently, it is directed through the turbine blades via the outlet to generate electricity. However, during drought conditions with minimal water levels, the hydropower ceases operation due to insufficient water supply. In cases when the inflow of water exceeds electricity production demands, the plant can switch to the reversible operation mode. Here, water is pumped from the main, lower reservoir to the upper reservoir until the upper reservoir reaches its maximum capacity.
The accumulated water is stored until it is required for electricity generation in the future. This process often involves utilizing the same turbines used for electricity generation, only now they operate as pumps to move water from the lower to the upper reservoir. When water inflow is low, and electricity demand is high, the operating mode "emptying the upper storage lake" can be initiated. In this scenario, water is discharged from the upper reservoir to the turbine blades, kickstarting electricity production by harnessing the stored potential hydropower within the reservoir.
During low electricity demand, water is stored in both reservoirs, potentially leading to reduced water levels downstream, endangering the ecosystem of the river. To maintain a minimum water level, careful control is essential. Conversely, during high inflow or flooding, overflow mechanisms such as special drains or additional pumps are utilized to prevent adverse effects.

4. TRAINING KIT STRUCTURE

A conceptual solution of suitable training kit for simulating various operating scenarios of PSH, like "Bajina Bašta," and potential cyber attacks on this CI is proposed in Figure 3. To enhance portability, the complete model is divided into two units housed in separate suitcases. Upon opening, these suitcases are placed side by side on a work table using internal mounting holders.
The left suitcase contains two reservoirs, labeled 1 and 2, representing the main, lower and upper reservoirs, respectively. The lower part of right suitcase features a larger reservoir labeled 3, representing the main river flow (natural body of water). A small 3D-printed turbine is positioned above reservoir 3, which rotates when water overflows from reservoirs 1 and 2 into the main stream. Capacitive sensors (labeled S1-S6) are installed in each reservoir to detect minimum and maximum water levels.
The proposed training kit for open-loop PSH, involves using electromagnetic 2/2 directional control valves (labeled R1 and R2) to control the flow of water from the lower and upper reservoirs (reservoirs 1 and 2,

respectively) to the turbine and the main stream of the river (reservoir 3) to simulate electricity generation. Pump P2 enables the water flow from the lower to the upper reservoir, while pump P1 is utilized for simulating the natural flow of the river in continuous mode by transferring water from the main stream (reservoir 3) to the lower reservoir (reservoir 1).

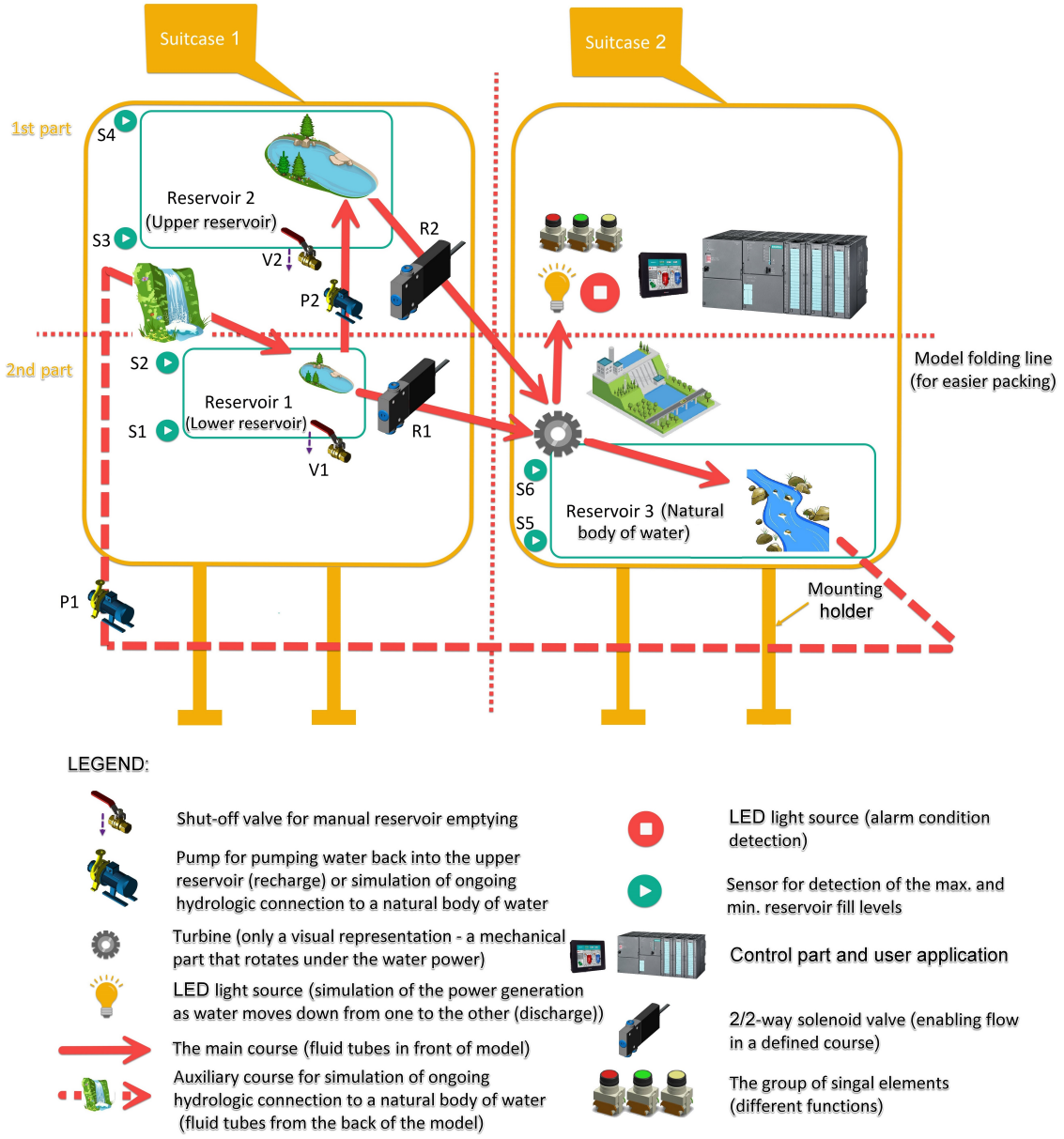

Figure 3: Conceptual solution of the open-loop PSH training kit

The control elements, including a PLC, HMI panel, two Modbus Remote Terminal Units (RTU), and a router, are placed in the upper part of the right suitcase. The PLC serves as the primary control device, while the HMI panel simulates a SCADA system for managing and monitoring the PSH operation. Modbus RTUs provide remote data transmission as sensors and actuators are located at remote points from the main control center in actual hydropower plants. Some sensors (S1-S4), pump P2, and directional control valve R2 are connected to one Modbus RTU, while pump P1 is connected to the second Modbus RTU to simulate the natural flow of the river (it cannot be the target of attack). Furthermore, sensors S5 and S6 and directional control valve R1 are directly connected to the PLC's inputs and outputs. The router enables communication among all the network devices and establishes a connection with the "outside world." Signal lamps, buttons, switches, and other control elements are used to simulate electricity production, system start/stop, and other operations.

Prior to closing the suitcase, it is necessary to manually activate shut-off valves V1 and V2 to drain water from reservoirs 1 and 2, respectively. In the next step, it is necessary to initiate the flow of water from

reservoir 3 through reservoir 1, activating pump P1, and discharging water outside using shut-off valve V1.

4.1 Normal operation mode

In the initial step of this scenario, pump P1 is activated to transfer water from reservoir 3 (representing the main river course after the dam) to the lower, i.e., the main reservoir (reservoir 1), simulating the water cycle. In the second step of this scenario, directional control valve R1 is switched on, releasing water onto the turbine to simulate normal electricity production.
However, for drought simulation purposes, pump P1 needs to be stopped. Additionally, if the water level in the lower reservoir (reservoir 1) reaches a minimum, indicated by sensor S1, or if other monitored parameters not included in the training kit necessitate it, pump P2 and/or directional control valve R1 must be turned off (if activated) to simulate the shutdown of the hydropower.

4.2 Reversible operation mode

The reversible mode can be initiated automatically when sensor S2 detects the maximum water level in the lower reservoir (reservoir 1), or manually based on other monitored parameters not included in the training kit. In this mode, pump P2 is activated, allowing water to flow from the main reservoir (reservoir 1) to the upper reservoir (reservoir 2). The process stops automatically when sensor S4 detects the maximum water level in the upper reservoir (reservoir 2) or manually based on other monitored parameters not included in the model.
In the training kit, for the sake of clarity and better comprehension of the process, the pump used for transferring water between the reservoirs (reservoirs 1 and 2) is separated from the turbine connected to the electric power generator. In reality, there is often only one turbine serving both purposes, generating electricity and facilitating water transfer between reservoirs.

4.3 Emptying the upper reservoir

In the course of implementing this scenario, directional control valve R2 is activated, initiating the release of water from the upper reservoir to the turbine blades. The activation can occur upon receiving a signal from the control level indicating the need for electricity production from the reserve. However, the process is automatically halted when a signal is received from sensor S3 indicating that the water level in the upper reservoir (reservoir 2) has reached a minimum, or based on monitoring other parameters not included in the training kit that lead to the same conclusion.

4.4 Filling and emptying of the lower course of the river

When the water level in the main stream of the river (reservoir 3) drops to a critical point that could endanger biological conditions, sensor S5 is triggered, and the "maintenance of the biological minimum" mode is automatically initiated. In this mode, directional control valve R1 is activated, utilizing part of the accumulated energy to maintain the water level necessary for preserving the biological conditions. Conversely, if there is a substantial inflow of water into the main, lower reservoir, leading to significant overflow into the river, or if there is a considerable increase in water level downstream, sensor S6 is triggered. This activation prompts the reactivation of pump P1, allowing excess water from the river drainage stream (reservoir 3) to flow back into the lower reservoir (reservoir 1).

4.5 Potential attacks

During the conceptual design of the training kit, the potential for various attacks on PSH was taken into consideration. In addition to the regular fluid connections and tubes for water flow in the mentioned scenarios, various "overflows" were predicted. For instance, in the event of an attack that would affect the maximum water level detection in the lower reservoir (reservoir 1) and upper reservoir (reservoir 2), leading to "false" signals from sensors S2 and/or S4, it is possible to redirect water through additional connections and tubes to the main stream of the river (reservoir 3). This simulation allows for the representation of an undesirable situation, where there would be a "reservoir overflow" scenario, while still ensuring the protection of the equipment and related components in the best possible manner. Other potential attack scenarios were also considered during the development of the training kit to ensure comprehensive evaluation and preparedness.

5. CONCLUSIONS

This paper presents the basics for the development of the training kits for examining and testing the CS of CI. The necessary conceptual requirements for the design of training kits are developed. The case study of conceptual design of a training kit for testing the CS of the open-loop PSH is given. Future research will be related to 3D modeling and physical realization of the mentioned training kit, programming of defined operating scenarios, and at the very end, testing of different types of malicious attacks.

ACKNOWLEDGMENTS

This research has been partially supported by the Ministry of Science, Technological Development and Innovation through project no. 451-03-47/2023-01/200156 "Innovative scientific and artistic research from the FTS (activity) domain".

REFERENCES

Chowdhury, N. & Gkioulos, V. (2021) Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review.* 40, 100361. Available from: doi: 10.1016/j.cosrev.2021.100361

Elektroprivreda Srbije. (2023-1) *HE Bajina Bašta*. Available from: https://www.eps.rs/lat/dlhe/Stranice/HE-Bajina-Basta.aspx [Accessed 19th July 2023] (in Serbian)

Elektroprivreda Srbije. (2023-2) *RHE Bajina Bašta*. Available from: https://www.eps.rs/lat/dlhe/Stranice/RHE-Bajina-Basta.aspx [Accessed 19th July 2023] (in Serbian)

Ghafir, I., Prenosil, V., Svoboda, J. & Hammoudeh, M. (2016) A Survey on Network Security Monitoring Systems. *Proceedings of IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, Austria.* pp. 77-82

Maglaras, L. A., Kim, K. -H., Janicke, H., Ferrag, M. A., Rallis, S., Fragkou, P., Maglaras, A. & Cruz, T. J. (2018) Cyber security of critical infrastructures. *ICT Express.* 4 (1), 42-45. Available from: doi: 10.1016/j.icte.2018.02.001

Službeni glasnik Republike Srbije, br. 87. (2018) *Zakon o kritičnoj infrastrukturi.* Available from: https://www.paragraf.rs/propisi/zakon-o-kriticnoj-infrastrukturi.html [Accessed 18th July 2023] (in Serbian)

Ten, C. -W., Manimaran, G. & Liu, C. -C. (2010) Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*. 40 (4), 853-865. Available from: doi: 10.1109/TSMCA.2010.2048028.

U. S. Department of Energy. (2023) *Pumped Storage Hydropower.* Available from: https://www.energy.gov/eere/water/pumped-storage-hydropower [Accessed 19th July 2023]

Viganò, E., Loi, M. & Yaghmaei, E. (2020) Cybersecurity of Critical Infrastructure. In: Christen, M., Gordijn, B. & Loi, M. (eds.) *The Ethics of Cybersecurity.* The International Library of Ethics, Law and Technology, vol 21. Springer, Cham, pp. 157-178.