Virtualization of the Experiential Learning Platform for Critical Energy Infrastructure using Digital Twin Technology and Cloud-based Applications

M. Manbachi*, M. Shariat-Zadeh*, M. Hammami*, I. Letvenchuk, H. Farhangi***
British Columbia Institute of Technology (BCIT)*, Siemens Canada Limited**
CANADA

SUMMARY

With the advent and the expansion of Industry 4.0 critical infrastructure technologies and applications such as Cloud-based systems, Internet of Things (IoT), Artificial Intelligence (AI), and Pervasive Analytic solutions, industrial companies, and utilities are recently becoming more interested in re-training their existing manpower with the advanced technologies or hiring experts from other industries to provide on-the-job hands-on training that can address skills gaps. The onset of COVID19, the need for physical distancing, and recent remote working routines have made such training programs difficult to offer. In particular, industries that require interdisciplinary teams to be trained with real critical infrastructure assets have suffered the most. Acknowledging the critical need for such hands-on training, BCIT's Critical Infrastructure Cybersecurity Laboratory (CICL), enables training of Canadian Utilities' workforce and students on new technologies required to keep Canada's critical energy infrastructure safe and cybersecure. In 2020, BCIT's Smart Microgrid Applied Research Team was granted funding by the Future Skills Centre to develop technology for digital twining, the replication of the control layers of physical assets, and moving control systems into cyberspace to enable remote access to physical devices. Thus, a new framework for virtualization of experiential learning, in the form of hands-on exposure to real systems, has recently been developed. This paper primarily introduces this platform, its capabilities, features, and functionalities. It then explains how virtual control layer stages can be defined. In the following section, the paper elucidates how the developed interface can provide a virtual environment for trainees using digital twin technology and cloud-based applications (e.g., dashboards and navigators), which allow trainees to remotely work with lab assets and components in real-time and receive online feedback. Following that, this paper describes how such virtualized platforms can be supported by selecting proper communication and networking protocols and systems. Last but not least, the paper lists potential cyberattacks on such platforms and presents an effective cybersecure topology. The results of this paper indicate a great potential for the utilized virtualization technology to be applied to other industrial and/or institutional digital experiential learning programs or virtualization platforms in which reliable and secure remote access to physical assets is required to support relevant experiential learning pedagogical models.

KEYWORDS

Digital Twin Technology, Virtualization, Experiential Learning, Cloud Monitoring, Substation Automation Systems, IEC 61850, Remote Access Technology, Cybersecurity.

mmanbachi@bcit.ca

INTRODUCTION

Vocational training schools constitute an essential component of Canada's educational system. Institutes such as BCIT have traditionally provided hands-on and practical educational programs, aimed at supplying Canada's industry with job-ready graduates. This type of training was largely based on the ability of these institutes to provide their students with the opportunity to work hands-on with the technologies, platforms, and assets found in the industry. COVID19 has diminished that ability. To accommodate social distancing, these institutes have reduced their student enrollments substantially or have begun offering some programs online. It may be acceptable to have a reduced student intake in trades programs that require students to handle certain assets on their own, however, other programs that require students to work as part of a team (e.g., system design, cybersecurity, etc) have suffered the most. These programs must provide the students and trainees with an online environment that allows them to work in multidisciplinary teams on real-life industry-grade assets and systems. Technologies such as Virtual Reality (VR) or Simulation engines aren't powerful enough to support hands-on experiential learning remotely or in cyberspace.

In recent years, many efforts have been made in the design and development of efficient virtualized platforms and/or reliable remote connections for online testing, operation and maintenance, and training of critical energy infrastructures such as digital substations. More often, they focused on Virtual Desktop Infrastructure (VDI) and Virtual Machine (VM) solutions and technologies for remote connection. For instance, an application control system that creates an efficient and protected VDI station has been presented in [1]. In [2], the authors used a secure paradigm pseudo-hypervisor IP-based virtualization technology that encrypts IP addresses and restricts unauthorized entries. In [3], a high-available and secure system has been created on the OpenStack cloud platform and implemented as a prototype system. In another work [4], hyper-Cache has been presented which makes a shortcut in QEMU open source emulator by intercepting I/O requests in the hypervisor.

In addition to VDI and VM-related works, some have extensively worked on the design and development of a virtual platform specifically for critical infrastructures such as digital substations. For instance, [5] builds an experiment platform for digital substations based on IEC 61850 to introduce substation automation into university experiment teaching. Here, MMS and Goose communication between the substation IEDs are simulated by IEDScout and libiec61850 software. In [6], a cloud platform based on DC bias monitoring and warning system that supports browser and mobile terminal access, data analysis, data display, early warning forecast, and data query service has been proposed. A bi-directional digital twin application has been developed at the University of South Australia [7] using OPC UA connection, NX siemens as a CAD simulation platform, and a SCADA system with python servers driven from inputs of the assembly cell. The simulation platform shown in [8] is a virtual reality simulation training system for substations based on CAD drawings. Last but not least, a virtual simulation platform has been proposed in [9] for substation auxiliary equipment.

From the literature, it can be concluded that only a few studies have been completed on the design and development of a reliable and secure experiential learning platform for critical energy infrastructure for hands-on training purposes. Through BCIT's virtualized experiential learning platform, the command and control layer of substation assets can be migrated into cyberspace while the assets themselves remain physically grounded. By doing so, trainees can interact with real-life systems securely and safely without being physically present in the lab. Furthermore, the greater impact of this approach would be that such training could be offered to individuals and communities across Canada and the globe. Next, BCIT's virtual experiential learning platform will be explained, including its background, features, and functionalities.

BCIT's VIRTUALIZED EXPERIENTIAL LEARNING PLATFORM

BCIT's Critical Infrastructure Cybersecurity Laboratory (CICL) has been designed and developed to provide a utility-grade real-time R&D platform, enabling researchers and educators alike to conduct research and educational programs in power systems, digital substations, smart microgrids, and critical infrastructure cybersecurity applications. The lab was so far built in partnership with the Department of National Defence, Siemens Canada, Future Skills Centre, and other utilities & industrial companies. This unique installation emulates the required power-flow layer of the desired SuT (System under

Test) using HIL (hardware-in-the-loop) emulation, while the command & control layers are implemented using the leading-edge components (relays, Merging Units (MU), etc.) from industrial partners. This provides the platform with a unique capability to be used for research, design, and validation of substation architectures, communication protocols, protection schemes, DER integrations, and what-if scenarios related to cyber-vulnerability and mitigation strategies of critical energy infrastructure. In particular, this real-time platform is designed to enable vulnerability studies of critical infrastructure, which includes provisions for initiating, observing, and mitigating various categories of cyberattacks on the grid. The platform uses the IEC-61850 communication protocol and emulates a fully functional medium voltage substation and a microgrid with various types of loads and Distributed Energy Resources such as PV, BESS, and EV chargers using a Real-time Digital Simulator (RTDS). RTDS enables the lab to fully implement three key levels of substation topology, i.e., process level, bay level, and station level. The lab includes real-field IEC 61850-compliant substation protection IEDs such as protection relays, MUs, and fault recorders. The lab is comprised of real-time monitoring and an HMI system that is able to control and monitor the whole system in real-time (Fig. 1).

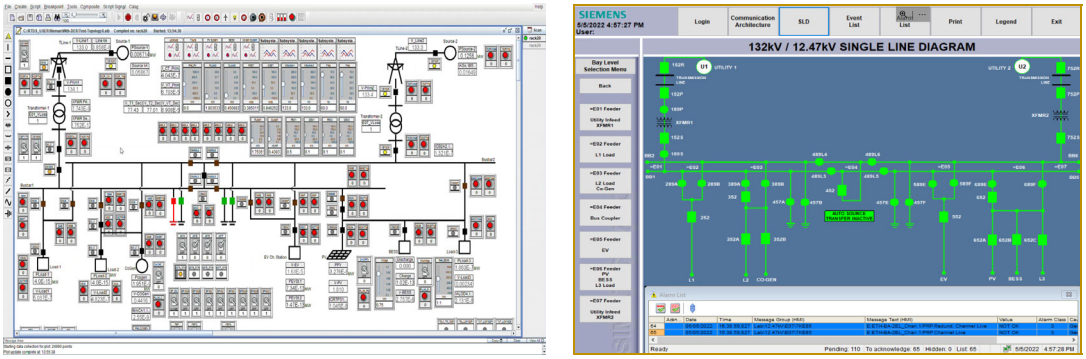

Fig. 1. left: CICL lab runtime monitoring platform, right: Industrial HMI

With the support of the Future Skills Centre fund [10], the CICL lab has been recently equipped with advanced virtualization technologies and cloud-based applications. These created a tremendous opportunity for the platform to be used for remote hands-on training purposes. Using advanced virtualization technologies such as digital twins, and cloud-based dashboard and navigator applications at the cyberspace layer connected to the real-field devices & systems, trainees are now able to get the same level of understanding and experience with physical assets even from their homes. By offering vocational training remotely, this platform adds substantial value to Canadian academic institutions, utilities, industries, and specifically to remote and underserved communities that might not have adequate resources to get involved in such training programs in person.

In summary, the following goals can be achieved using this test platform: design and validation of architectural choices for IEC 61850 compliant substations and smart microgrids, providing professional in-person and remote training and educational programs for students and scholars on critical energy infrastructure, conducting real-time testing, validation, and emulation of MV substations and smart microgrid operations using hardware-in-the-loop system, examining advanced substation automation, networking application solutions and protocols, conducting interoperability tests of various protection schemes by mixing and matching different components and IEDs from various vendors, and offering studies and training opportunities (in-person and online) on critical infrastructure cybersecurity (e.g., understanding and analysing potential vulnerabilities and cyber threats to North American critical smart grid infrastructure, disseminating the knowledge and findings within the community and in particular with Canadian research institutes and utilities, developing, testing, and validating mitigation and early warning system solutions and technologies against cyber vulnerabilities, studying cybersecurity measures: availability, integrity, privacy, authentication, authorization, auditability, and non-repudiation, providing general and customized training programs for students, utility personnel, and other interested parties on critical energy infrastructure cybersecurity issues and mitigation strategies and technologies, and facilitating the development of

best practices and cybersecurity regulations to increase Canada's infrastructure's defense potency against cyberattacks).

Three clusters of activities have been proposed to provide trainees with a reliable and secure virtualized hands-on training platform:

1. To facilitate remote access to physical assets, the command and control layer of the physical assets was replicated digitally and moved into cyberspace. For this purpose, virtual control layers were developed, capable of coexisting with the actual control layers of the physical assets in the lab. Additionally, the hardware-in-the-loop platform that emulates the substation's bulk components was upgraded to support multiple simulation sessions.

2. Establishing secure remote access to the substation's lab for cohorts/teams, allowing team members to collaborate securely in cyberspace on various operational aspects. By utilizing a virtual dashboard, trainees can manipulate control and protection strategies in real-time, and receive instantaneous feedback from the lab assets for their commands/actions.

3. Piloting the developed platform through an actual training program. The platform will conduct a focused pilot session with a small number of students to ensure the sustainability of the system change it advocates. As part of the pilot, the performance parameters of the platform will be optimized for hands-on training on such assets. The results of this pilot will also be used to optimize use cases, instructional materials, and pedagogical models.

Last but not least, the entire platform is going to be integrated into BCIT's Learning Management Systems (LMS). Integration with BCIT's LMS makes the platform readily available to many online training programs, which BCIT currently offers to students and professionals. Many training programs require remote access to such assets for practical work and hands-on learning. Fig. 2 shows CICL's virtualized experiential learning approach for individual and group-based course modules.

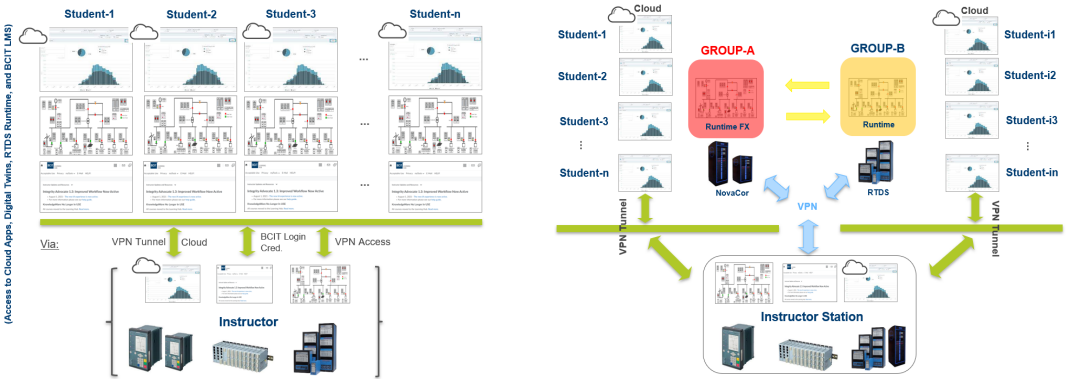

Fig. 2. CICL's approach for virtual hands-on training (left: individual-based modules, right: group-based modules)

TOOLS FOR THE VIRTUALIZATION OF SUBSTATIONS

Generally speaking, the following tools and technologies are needed for the virtualization of MV substations:

- Hardware-in-the-loop real-time simulator/emulator to model and co-simulate the electrical circuits and control logics
- Monitoring and diagnostic platform and/or application
- Remote access controller and HMI
- The digital twin of the existing assets
- Cloud for hosting data, applications, and data optimization
- Cybersecurity tools to ensure the platform is cybersecure, etc.

For hardware-in-the-loop simulation and real-time emulation, BCIT's virtualized experiential learning platform uses RTDS (including processing and networking cards that support IEC 61850 and other substation protocols) and NovaCor technologies. For monitoring, control, and diagnostic, the platform not only utilizes an industrial HMI but also uses an RTDS runtime monitoring platform (Fig. 1).

Moreover, the platform has been equipped with three new cloud-based applications that can be used for monitoring and analysis purposes; SIPROTEC Dashboard, SICAM Navigator, and Distributed Energy Optimizer (DEOP).
These cloud-based applications virtualize the operation of digital substations for users. A SIPROTEC Dashboard presents an overview of the status of SIPROTEC devices as well as a map view, that shows where they are located in the field in relation to SIPROTEC devices. Additionally, the dashboard implements virtualization and download options as well as fault information across the entire grid. The SIPROTEC system allows monitoring of protection settings as well as visualizing log files related to devices. Additionally, the dashboard can be accessed on mobile devices and SMS notifications can be sent. As a novel virtualization strategy, it also implements improved navigation breadcrumbs (which improve the monitoring of SIPROTEC devices' operational status and optimize their O&M). In addition, it is also used to monitor SIPROTEC devices and improve grid transparency (including the status of protection relays). Users are notified of abnormal device operations such as protection trips and pickups. Fig. 3 shows, CICL'S dashboard implementation.

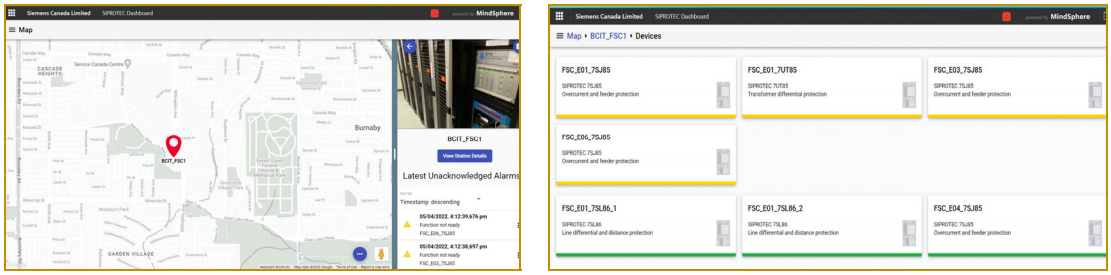

Fig. 3. left: CICL's dashboard map and acknowledgment alarms, right: dashboard showing IED status

The SCIAM Navigator is used with the SICAM A8000 RTU as a grid edge device to monitor transformer substations, optimize maintenance, and reduce outages. Using the GridEdge node, devices can communicate with MindSphere through the standardized OPC UA Pub-Sub Protocol. With the SCIAM Navigator, no additional hardware extensions or engineering processes are required, and mobile and desktop interfaces are available. The Navigator also provides in-depth monitoring of medium and low voltage networks as well as secondary distribution substations. Geolocation views of transformer substations, along with context-aware markers, are implemented in its grid view. Active fault indications across the grid can be viewed in a list view, with email notifications provided. The station view provides a station topology, fault direction indicators as well as blown-fuse alarms. Fig. 4 depicts implemented navigator in the CICL. Last but not least, DEOP is a cloud-based software helping Energy Service Companies (ESCO), aggregators, campuses, industrial players, utilities, EPCs, and IPPs to improve performance and increase profitability [11].

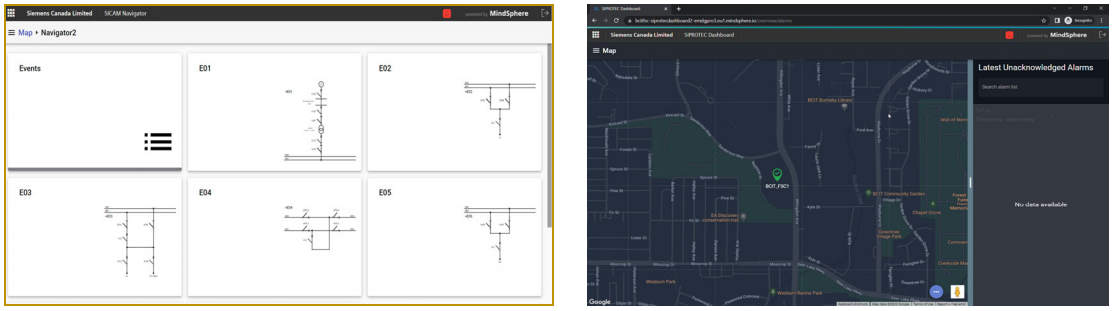

Fig. 4. left: Substation section SLDs showing breaker status, right: CICL's SICAM Navigator and acknowledged alarms

In order for trainees to gain hands-on experience on protection relay configuration, IEC 61850 Goose communication, and other protection system studies, SIPROTEC digital twins technology is used in the proposed platform. The SIPROTEC digital twin is a digitally virtualized copy of the SIPROTEC-5. The digital twin provides a reliable method of testing SIPROTEC-5 devices in terms of efficiency, performance, security, and 24/7 availability. The SIPROTIC digital twin features a front display that allows users to navigate menus, use function keys, and more. A current injection, voltage injection, or

binary input can be used to trigger protection trips. In addition, it can be used to test protection features, automation logic, and customer-specific applications, as well as to train the SIPROTEC-5 intuitively. It also includes IoT-Applications. IEC 61850 communication GOOSE messaging protocol is used to communicate between devices (such as interlockings). A series of Ethernet protocols, including IEC 61850, DNP3, Modbus, TP, and IEC 60870-5-104, can be used to test the integration of the following substation automation systems: SICAM A8000, SICAM PAS/SCC, and SCADA systems. Additionally, the twin examines faults (e.g., a replay of records) and tests cybersecurity functions (e.g., Syslog, RADIUS). Fig. 5 shows the final structure of the proposed experiential learning platform including SIPROTEC digital twins.

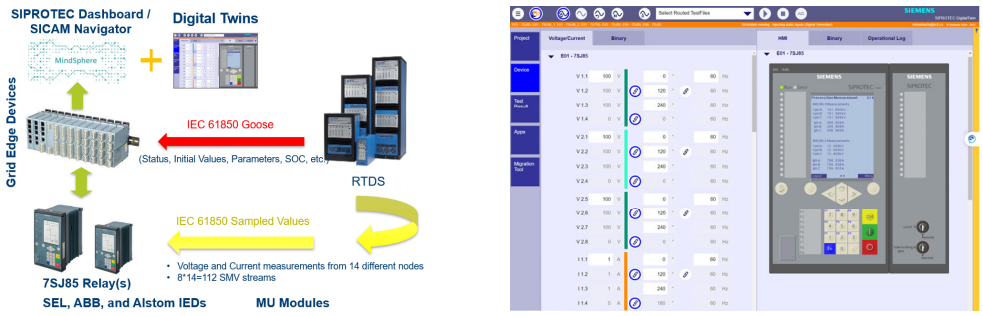

Fig. 5. left: topology of the virtualized experiential learning platform, right: SIPROTEC digital twin using IED's SIM file.

In addition to the abovementioned equipment and systems, BCIT's CICL platform uses other equipment such as omicron V/I, more than seven protection relays and MUs from different vendors, a fault recorder, a PRP-based communication network architecture, a microgrid controller (MGC), a GPS antenna and a clock for full synchronization. The CICL lab is also equipped with required tools for cybersecurity studies such as IEC 61850 Avenue, IEC 61850 Toolset, Goose Injector, SMV Injector, RTDS, and an AI-based Early Warning System that enable simulating cyberattacks and support cyber threat studies. To ensure the security of the system, the Claroty IDS and its associated firewall is going to be installed and configured soon. In conclusion, the developed platform is equipped with proper tools and technologies for substation automation virtual hands-on training.

PROPOSED COMMUNICATION AND CYBERSECURITY ARCHITECTURES

In order to develop a reliable network for the virtualized experiential learning platform, a PRP-based network was implemented with two different LAN systems. Fig. 6 shows the communication architecture of one of the LANs. Moreover, to adapt the old environment to the new cloud-based system, several works and upgrades such as updating process bus modules, upgrading IEDs' firmware, installing new Ethernet switches and redundancy boxes, upgrading software tools, and installing SFP modules & new redundant network access were completed. To balance networking traffic, we segregated IEC 61850 messages by moving SMV streams to a separate VLAN.

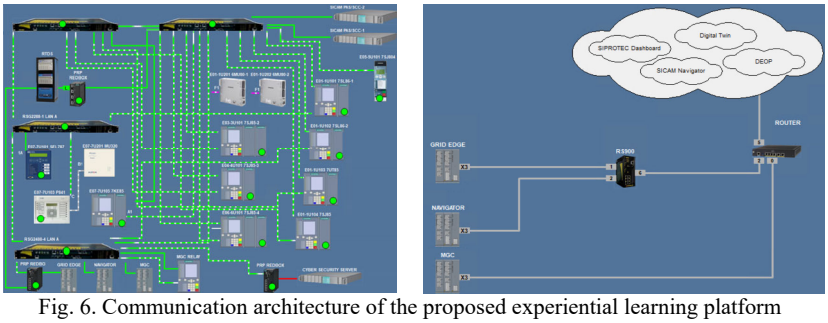

Fig. 6. Communication architecture of the proposed experiential learning platform

The CICL's Lab approaches cybersecurity with a deep understanding of the impacts of various possible cyberattacks. The cybersecurity procedure was derived from leading industry standards

including ISO 27001 (Security Management), IEC 62443, and ISO 31000 (Risk Management). The security analysis and assessment activities were kept aligned with industry-acknowledged methodologies such as penetration testing execution standard which we offered in form of red/blue team type of exercise scenarios, NIST SP 800-115, and Technical Guide to Information Security Testing. As one of the first steps, potential attacks on digital modern substations were studied thoroughly. This includes not only the conventional IT-related attacks but also protocol-based and component-based attacks such as IEC 61850 Goose forgery (when a forged Goose message leads to mal-operation of breakers or earth switches or causes forged breaker failure condition), SMV forgery by changing V/I measured values, Goose avalanche (that may congest network's bandwidth), HMI hijack (through MMS forgery or direct IT-based attacks), reverse polarity of DR/DER sources (through protocol-based attacks), disable protection function, relay setting tampering, sensitive pickup protection, shift SMV timestamp to trip differential protection and uncalibrated gain (CT ratio) of the current measurement. More information about potential vulnerabilities and listed cyber threats to such infrastructure can be found in [12].

Fig. 7 presents the architecture of the virtualized experiential learning platform. As shown in this figure, the proposed architecture includes two servers located at the demilitarized zone with a Claroty solution that is comprised of a continuous threat detection (CTD) and an Enterprise Management Console (EMC). The CTD encompasses both IT & OT parts of the platform. It supports network segmentation, anomaly, and threat detection, OT monitoring, asset management, vulnerability and incident management, data management, and control. The EMC is utilized for analytics, reporting, alert management, and multi-site CTD deployments. It can also be deployed in the Claroty Cloud through a SaaS-based approach. To further protect the platform against intruders, an APE firewall with proper rules sits between the cybersecurity servers and IT/online services.

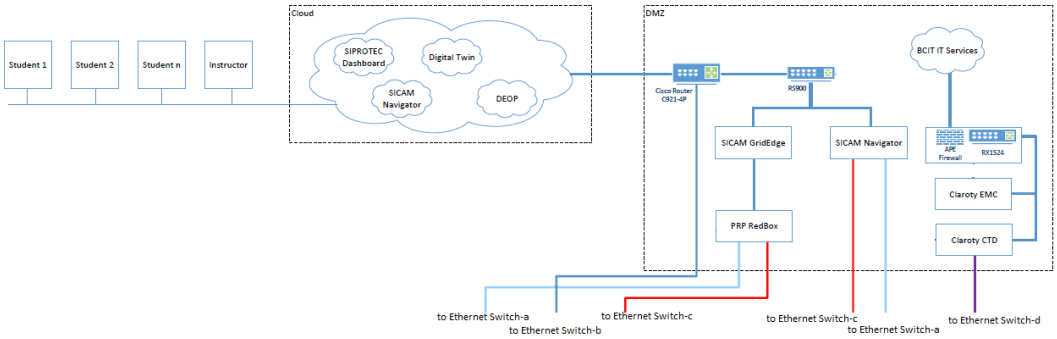

Fig. 7. Cybersecurity architecture for the virtualized experiential learning platform

CONCLUSIONS

With the recent pandemic, the need for virtual learning arises and many efforts have been made to develop transformational technologies, solutions, and methodologies to replicate the same quality, efficiency and scale, required for experiential learning within cyberspace, while keeping the physical assets intact. The proposed project presented an important body of knowledge on how to create and support efficient and cybersecure experiential learning opportunities for trainees in the wake of social or physical restrictions imposed by abnormal events. Although this project dealt with a very specific domain of critical energy infrastructure, the body of knowledge that it created could be beneficial for other domains as well; in particular, methodologies to migrate the command and control layer of the physical assets to cyberspace and provide safe and secure access to trainees for "learning by doing". The primary objective of the proposed methodology was to enable the trainees to acquire the same set of experiences and learnings as the real target environment. After the development phase (which is almost completed), and once proper pedagogical models are developed, proven, and streamlined, the body of knowledge could be correspondingly utilized in other domains, where experiential learnings are equally important. The developed platform explained in this paper now opens up this type of training to all those who would like to be trained, including academic students, industrial experts, under-served communities, recent immigrants, first nations and remote communities, and those who would like to be re-trained.

ACKNOWLEDGMENT

«Virtualization of Experiential Learning Platforms and their Pedagogical Models is funded by the Government of Canada under the Future Skills program».
«Virtualisation des plateformes d'apprentissage expérientiel et de leurs modèles pédagogiques est financé par le gouvernement du Canada dans le cadre du programme Compétences futures».

BIBLIOGRAPHY

[1] A. Algawi, M. Kiperberg, R Leon, A Resh, N. J. Zaidenberg, "Efficient Protection for VDI Workstations" (2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), June 2019, Paris, France)

[2] K M. Babu, P Sai Kiran, "A secure virtualized cloud environment with pseudo-hypervisor IP based technology" (2nd International Conference on Next Generation Computing Technologies (NGCT), October 2016, India).

[3] W. Zhan, L. Ruan, X. Yue, Z. Xu, L. Xiao, "A Secure and VM-supervising VDI System Based on OpenStack" (7th International Conference on Cloud Computing and Big Data (CCBD), July 2017, Macau, China).

[4] T. Kim, S. Choi, J. No, S. S. Park "hyperCache: A Hypervisor-Level Virtualized I/O Cache on KVM/QEMU" (Tenth International Conference on Ubiquitous and Future Networks (ICUFN), July 2018, Prague, Czech Republic).

[5] Q. Fu. J. Chen, "Design of experiment platform for digital substation based on IEC 61850" (5th International Conference on Computer Science and Network Technology (ICCSNT), October 2017, Changchun, China).

[6] W. Wu, L. Li, "Design and Application of DC Bias Monitoring System Based on Cloud Computing" (5th IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS), April 2019, Nanjing, China).

[7] A. Protic, Z. Jin, R. Marian, K. Abd, D. Campbell, J. Chahl "Implementation of a Bi-Directional Digital Twin for Industry 4 Labs in Academia: A Solution Based on OPC UA" (IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), December 2020, Singapore).

[8] X. Liao, J. Niu, H. Wang, B. Du "Research on Virtual Reality Simulation Training System of Substation" (International Conference on Virtual Reality and Visualization (ICVRV), October 1017, Zhengzhou, China).

[9] Y. Qi, M. Tian, X. Chen, P. Huang, "Design and Research of Virtual Simulation Platform for Substation Auxiliary Equipment" (5th Asia Conference on Power and Electrical Engineering (ACPEE), June 2020, Chengdu, China).

[10] Future Skills Centre, "Virtual learning in Canada's infrastructure sector", [Online]: https://fsc-ccf.ca/projects/virtual-learning-infrastructure-sector/

[11] Unlock the value of your distributed energy resources with DEOP; Improve performance, increase profitability, [Online]: https://new.siemens.com/global/en/products/energy/energy-automation-and-smart-grid/grid-edge-software/deop.html

[12] E. Hawthorne, M. Manbachi, A. Gilani, "Substation Anomaly Detection System – A Substation & Distribution Network Cybersecurity Early Warning System" (CIGRE Canada Conference & Expo, CIGRE-226, September 2019, Montreal, Canada).