FSC Project - Final Report (Concise Version)

Virtualization of the Experiential Learning Platforms and Their Pedagogical Models

Prepared by:

BCIT

SMART (Smart Microgrid Applied Research Team),
Centre for Applied Research and Innovation,
British Columbia Institute of Technology

Report to: Future Skills Centre (FSC)

March - April 2023 (Concise Version Prepared for FSC - April 2024)

This report was produced as part of a project funded by the Future Skills Centre (FSC), with financial support from the Government of Canada's Future Skills Program.

FSC is a forward-thinking centre for research and collaboration dedicated to preparing Canadians for employment success. We believe Canadians should feel confident about the skills they have to succeed in a changing workforce. As a pan-Canadian community, we are collaborating to rigorously identify, test, measure, and share innovative approaches to assessing and developing the skills Canadians need to thrive in the days and years ahead. The Future Skills Centre was founded by a consortium whose members are Toronto Metropolitan University, Blueprint ADE, and The Conference Board of Canada

The opinions and interpretations in this publication are those of the author(s) and do not necessarily reflect those of the Future Skills Centre or the Government of Canada.

Future Skills Centre
Centre des Compétences futures

Canada

Table of Contents

Summary

Background and Description:

The Critical Infrastructure Cybersecurity Laboratory (CICL) [1] at BCIT was designed and developed to serve as a utility-grade, real-time R&D platform, to support utilities, vendors, researchers, and educators to conduct research and training on critical energy infrastructure such as power systems, digital substations, smart microgrids, and operational technology cybersecurity. This installation uses a hybrid cyber-physical system where the power system layer of the SuT (System under Test) uses hardware-in-the-loop (HIL) emulation, while the command & control layers are implemented using physical assets (such as relays, multifunction units, etc.) provided by leading industrial partners. This provides the platform with a unique capability for training, research, design, and validation of substation architectures, communication protocols, protection schemes, DER integrations, and what-if scenarios pertaining to cyber vulnerabilities and mitigation strategies for critical infrastructure. In particular, the real-time platform is designed to assess the cyber vulnerability of critical infrastructure, including the initiation, observation, and mitigation of various categories of cyberattacks on national grids, as well as the monitoring and mitigation of those incidents. As the national and international concern for the cyber safety of critical infrastructure is increasing, this unique implementation is a significant step forward to increase cyber assessment as well as mitigation capabilities.

The CICL platform uses the international standard IEC 61850 communication protocol, to mimic a fully functional medium voltage substation and a grid-connected microgrid with a wide range of loads and Distributed Energy Resources (DERs) such as PV, Battery Energy Storage System (BESS), and Electric Vehicle (EV) chargers. A Real-Time Digital Simulator (RTDS) system and its Digital Twin (DT) models enables the lab to fully implement three key levels of substation topology, i.e., process level, bay level, and station level. The environment integrates real devices used for substation protection and control of Intelligent Electronic Devices (IEDs) such as protection relays, merging units, and fault recorders using IEC 61850 Generic Object-Oriented Substation Event (GOOSE), Sampled Measured Values (SMVs), and Manufacturing Messaging Specification (MMS) protocols. This lab includes both real and digital twin versions of a Human Machine Interface (HMI) system that can control and monitor the whole system. As a result, the lab environment represents a realistic digital twin with a realistic energy system and the latest control and protection devices directly integrated.

With the arrival of COVID, it became important to allow remote use of the lab capabilities for teaching, training, and research. With the support of the Future Skills Centre project in 2021-2022 [2], the CICL lab has been equipped with highly advanced virtualization technologies and cloud-based applications which led to the creation of an advanced Virtualized Experiential Learning Platform called "VELP". Consequently, this platform provides an excellent opportunity for remote hands-on training, which opened up a number of new possibilities beyond academic research.

Using digital twins, and virtualization tools trainees are able to gain an in-depth understanding and experience of physical assets remotely, even when connected from their homes. By offering vocational training remotely, CICL lab offers great value to Canadian academic institutions, utilities, industries, and specifically to remote and underserved communities that might not have adequate resources to participate in such training programs in person. The following research, teaching, and learning activities can now be conducted using this platform:

- Remote and in-person professional training for utility operations, control, and protection topics
- Cyber threat scenario creation and table-top exercises for mitigation

- IEC 61850-compliant design and studies for digital substations and smart microgrids
- Development of infrastructure digital twins and hybrid cyber-physical systems using RTDS
- Verification of performance and product designs of new IED and relay devices.
- The applications for the platform's features supporting remote training on topics that require experiential learning are end less. Some examples include:
    - Providing general training programs for students, utility personnel, and other interested parties on critical energy infrastructure cybersecurity issues and mitigation strategies and technologies
    - Customized training for utility staff in identifying and responding to critical cyber scenarios.
    - Creating a periodic refresh program to ensure the latest cyber threats are communicated to utility operating personnel.
    - Understanding and analyzing potential vulnerabilities and cyber threats to North American critical energy infrastructure and advising vendors that may have unknown vulnerabilities.
    - Developing, testing, and validating mitigation strategies and/or early warning system solutions as well as technologies for detecting cyber threats/vulnerabilities
    - Facilitating the development of best practices and cybersecurity framework compliance to increase Canada's infrastructure's cyber-defense potency against cyberattacks.
    - Disseminating the knowledge with the community of experts and in particular with Canadian utilities and institutes

The Need

The onset of the pandemic and the need for physical distancing had forced many post-secondary institutions to move their academic and educational programs online. While some subjects lend themselves well to online/remote instruction, vocational training constructed based on experiential learning has been severely impacted. In particular, industries, which require training programs on real assets by interdisciplinary teams, have suffered the most. The critical Infrastructure sector faced specific concerns, in which the workforce needs to be trained together, and in teams, on "utility-grade assets and systems" and learn hands-on how to operate, maintain and protect these systems against cyberattacks. Recognizing the critical need for such training, BCIT's CICL enables the training of Canadian Utilities' workforce on new technologies required to keep Canada's Critical Infrastructure safe and cybersecure. Unfortunately, COVID-19 restricted physical access to the lab's assets for hands-on training and disrupted experiential learning programs, this led to the CICL pivoting to a fully remote virtualized implementation to preserve the experiential learning environment.

This project could successfully address these barriers by keeping the physical assets intact while virtualizing access to the training platform. The innovative Virtualized Experiential Learning Platform [3] removed the need for trainees' physical presence in the lab while allowing them to interact with actual utility-grade critical energy infrastructures in real-time as if they are in close proximity to such assets.

Project Approach

To address gaps and needs, we started with building a collaborative environment with our industry partner with the support of FSC. As a result of an extensive literature review, and technical discussions with our industry partner, the team determined that the best approach was to complete four activity clusters:

- First, migration of the command-and-control layer of the physical assets into the cyber-space, thus allowing remote access to the physical devices and systems.

- Second, developing secure remote access to the lab for cohorts/teams, enabling a secure collaborative platform for users working together. This type of interface provided a virtual dashboard for trainees, enabling them to manipulate various real-time control and protection strategies for the lab components, while also providing them with instantaneous feedback from physical assets for their commands/control actions.
- Third, piloting the developed platform with a selected team of trainees. In this cluster, several pedagogical models were studied to see which ones are more effective in facilitating remote experiential learning for adults. The platform's training content was also integrated into BCIT's Learning Management System.
- Finally, we planned for knowledge mobilization through holding workshops, training sessions, webinars, seminars, and publishing technical papers to share the outcomes of the project and learning achieved in developing a safe and secure virtualized experiential learning platform.

Key Testing Targets

The key aim of this project was to develop a virtualized experiential learning platform suitable for remote hands-on critical energy infrastructure training programs such as power systems, smart microgrids, and advanced digital substations. First, the project investigated how to migrate control and command signals into cyberspace effectively, reliably, and securely and how to test such signals traversing between physical assets and the cloud. Second, the project investigated effective solutions for remote experiential learning and teaching such as digital twins, real-time co-simulation, and cloud-based applications for monitoring, analysis, and cybersecurity studies. The third part of the project investigated methods of integrating multiple types of tools and technologies under one roof and bringing them into one place. Further, the project examined how to allow users to work as a team remotely and provide reliable remote access. As part of the evaluation plan, we tested both the technical performance of the platform and the technical efficacy of the remote sessions. To ensure the platform's performance, reliability, flexibility, and cybersecurity, several integration and verification tests were conducted. For testing purposes, pilot sessions with a limited number of students were held. Last but not least, the project proposed the best pedagogical models for developing experiential learning training modules and practices.

Target Groups/Populations to Serve

This project aimed to primarily serve BCIT students to receive virtual hands-on experience through the developed VELP. In addition, groups/populations shown in Table A are now able to join training programs/sessions and benefit from the developed platform as well:

Table. A. Project's Long-Term Audience

Group	Description
Canadian Universities/Institutes	Those interested in using VELP for virtual hands-on training
Canadian Research Institutes	Those who aim to conduct research in critical energy infrastructure studies
Remote Communities	Remote communities who seek basic or specialized education in substation, smart microgrids, and critical infrastructure cybersecurity
Utility Companies	Utilities that want to train their staff/workforce in the areas such as IEC 61850 substations and ICS cybersecurity
Industrial Companies	Product or services firms that want to train their staff/workforce in the areas such as substation automation, smart microgrid modeling, IEC 61850 substations, and critical infrastructure cybersecurity.
Newcomers	Job seekers and newcomers that would like to get trained on advanced critical infrastructure and join the job market

1. Introduction: BCIT's Virtualized Experiential Learning Platform

With the support of the Future Skills Centre and our industry partner, Siemens Canada, BCIT has successfully developed an advanced Virtualized Experiential Learning Platform (VELP) at CICL (located in BCIT's Burnaby Campus) to offer remote virtualized experiential learning, often in the form of hands-on exposure to real systems and physical assets by trainees individually or in teams. Using advanced virtualization tools and technologies (that are explained in detail later in this chapter of the report), integrated with real-field components and systems, trainees are now able to receive hands-on training remotely on different critical energy infrastructures such as substations and smart microgrids. As such, VELP could be of substantial value to Canadian academic institutions, utilities, industries, and remote communities that would like to receive training remotely or receive hands-on experience on recent advanced critical energy infrastructure and cybersecurity technologies and solutions. This chapter introduces VELP developed in this project, its features, functionalities, main architecture, assets, systems, and applications.

1.1 Critical Infrastructure Virtualization using VELP's Digital Twin Models

BCIT's VELP became a platform that enables virtualizing the operation of different critical energy infrastructure components such as substations, energy hubs, smart microgrids, and control systems. Virtualization is a well-established computing framework where the users are able to access physical resources over a cybersecure network, without being present on-site where the assets are. The platform includes two hardware-in-the-loop real-time simulators used for modeling energy infrastructure and emulating various operating scenarios online. This platform is also connected to real-field Intelligent Electronic Devices (IEDs), e.g., protection relays and merging units, that are used to protect the infrastructure against abnormal events (e.g., line-to-ground, line-to-line faults, and other failure conditions). The digital twins of various protection relays are now available in the cloud, which helps trainees understand such IEDs operate or can be configured. Different microgrid models are connected to a cloud application through an industrial microgrid controller as well so that trainees can work with real microgrid models, e.g., grid-connected, off-grid, and totally off-grid, and their various operating scenarios remotely. For example, SIPROTEC Dashboard and SICAM Navigator cloud applications are used to monitor and analyze substation data.

Through these cloud applications, trainees can monitor advanced substation components such as circuit breakers in semi-real time and use historical data for analysis purposes such as testing the operational performance of an advanced digital substation at different times of the year.

A visualization platform was also developed which is also available for training students. This presents trainees with 3D images of different physical substation components. VELP also includes Cyber-Threat Detection system not only to keep itself cybersecure but to provide an effective environment for trainees to learn more about such cybersecurity solutions and/or systems and understand how these solutions could protect critical energy infrastructures against cyber threats. Fig. 1.1 shows the main architecture of VELP developed in this project.

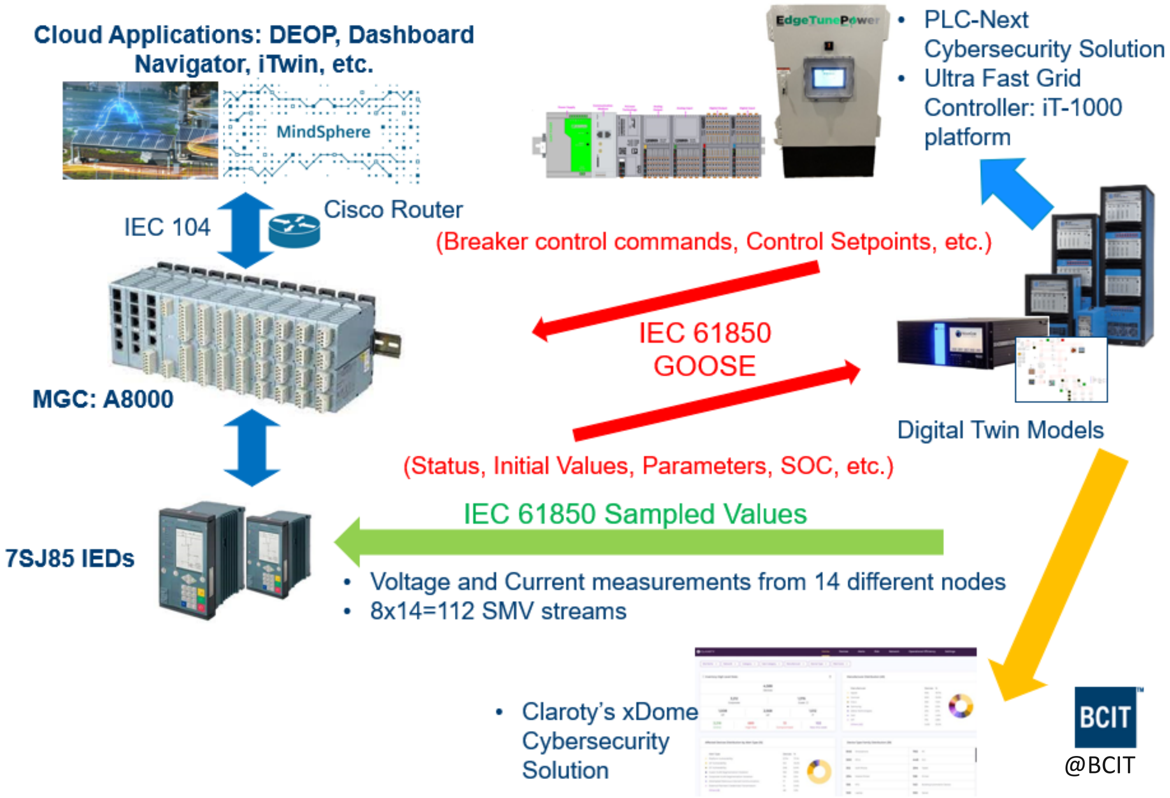
Cloud Applications: DEOP, Dashboard Navigator, iTwin, etc.
MindSphere
EdgeTunePower
• PLC-Next Cybersecurity Solution
• Ultra Fast Grid Controller: iT-1000 platform
IEC 104
Cisco Router
(Breaker control commands, Control Setpoints, etc.)
IEC 61850 GOOSE
MGC: A8000
Digital Twin Models
(Status, Initial Values, Parameters, SOC, etc.)
IEC 61850 Sampled Values
7SJ85 IEDs
• Voltage and Current measurements from 14 different nodes
• 8x14=112 SMV streams
• Claroty's xDome Cybersecurity Solution
BCIT
@BCIT

Fig. 1.1. The main architecture of BCIT's Virtualized Experiential Learning Platform (VELP) developed in this project.

- **Advanced Digital Substations:** Through its comprehensive real-time co-simulation platform, BCIT's VELP is able to support substation automation protocols such as IEC 61850 GOOSE (Generic Object-Oriented Substation Event), Sampled Values (SV) & Manufacturing Messaging Specification (MMS), DNP 3, and Modbus. The platform can be enhanced to include other industrial control protocols in the future as well.
- **Smart Microgrids:** BCIT transformed its smart microgrid training program from an on-site hands-on training system into an online and remote hands-on training environment [4]. The VELP includes an industrial microgrid controller that supports three different microgrid models with various microgrid topologies and operating scenarios such as off-grid microgrid that might suite remote communities, as well as grid-tied microgrids including various renewable energy resources such as batteries, solar panel, and wind turbines, for urban applications.
- **Other Energy/Grid Infrastructures:** BCIT's VELP also supports virtualized models of other critical energy infrastructures such as Energy Hubs, Battery Energy Storage Systems (BESS), Single busbar substations, and EV charging stations. These models are run in real-time for different training purposes such as cybersecurity, Operation & Maintenance (O&M), protection, Fault Location, Isolation, and System Restoration (FLISR).
- **Critical Energy Infrastructure Cybersecurity:** To assess cyber vulnerabilities in ICS protocols, BCIT's VELP team developed a cyber-physical simulation model that interacts with the virtualized models. Through the use of real-time simulations of physical assets of power systems, the models form a digital twin that is a cyber-secure virtualized platform to provide hands-on training in ICS cybersecurity, smart microgrids, and digital substations.

1.2 Virtualized Experiential Learning Platform Components

This section explains the key components BCIT's VELP uses in more detail. Understanding these components help readers understand how virtualized experiential learning platforms such as VELP use different components, tools, and technologies for remote vocational training.

- Real-time Digital Simulator: Real-time Digital Simulator (RTDS) is a powerful tool for modeling and simulating power and energy systems in real-time. Different types of grids and components are modeled and simulated using the RTDS software, RSCAD.
- NovaCor Technology: The NovaCor simulation hardware is the latest technology from RTDS. VELP uses four computational cores to enhance digital twin modeling capability.
- Human Machine Interface (HMI): For monitoring and control, the platform uses two real-time HMI systems: an industrial HMI from Siemens and a real-time monitoring platform created in the RTDS runtime (see Fig. 1.2; a runtime example for substation digital twin model).
- Digital Twins of Intelligent Electronic Devices: In the digital twin approach, real-time data is collected, models are created, and other data is recorded as part of the operation and service process of a physical asset during both the operations and the service process. It is a promising way of bringing the control and command layer of a physical asset into a virtual network when it is integrated with artificial intelligence or data analysis/prediction systems.

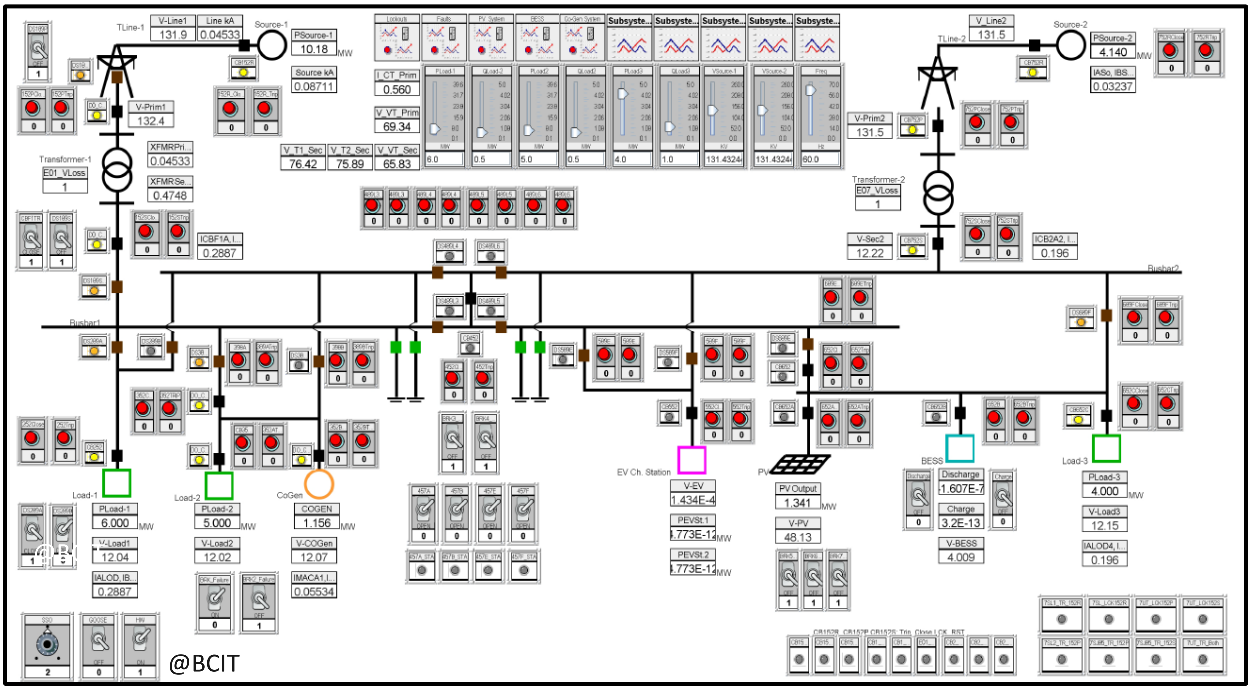

Fig. 1.2 Digital Twin model (created in RSCAD) for CICL's substation.

The SIPROTEC Digital Twins cloud application is used in the developed VELP to teach trainees how protection schemes can be set and how IEDs can be configured to support protection schemes. Hence, BCIT's CICL lab provides a virtual copy of SIPROTEC-5 devices (i.e., IEDs) that are physically present in the CICL lab. Through the cloud application of the digital twin, trainees can perform studies and tests such as IEC 61850 messaging, interlocking, IED integration, fault analysis, and cybersecurity to get familiar with IED configuration and operation [5].

- Data Monitoring and Analysis Cloud Applications: The platform currently uses four advanced cloud-based applications for monitoring, control, protection, and cybersecurity purposes.
- Threat Detection Solution: VELP currently uses one of the latest cybersecurity solutions from Claroty called the xDome which helps users become familiar with threat detection and monitoring solutions.
- Microgrid Controller: For microgrid training programs, the platform uses an advanced microgrid controller to enable a local real-field operational environment for developed digital twin models in VELP.
- Other Hardware Tools: A variety of vital energy infrastructure studies can be conducted with BCIT's VELP, which contains other advanced hardware tools such as HomerPro, RETSCreen, GAMS, and MATLAB. Depending on the training content, these components, and systems can be used for different critical infrastructure training purposes.
- Microgrid and Substation Visualization: The iTwin platform is used by VELP to enable students to become familiar with microgrids and substations virtually. The 3D models of substations and microgrids were also used for training modules.

1.3 VELP’s Communication Architecture

To build a reliable network for the virtualized experiential learning platform, a Parallel Redundancy Protocol (PRP) network was implemented using two different Local Area Networks (LANs). In addition, several works and upgrades were performed to adapt the old environment to the new cloud-based system, including updating process bus modules, upgrading IED firmware, installing Ethernet switches and redundancy boxes, upgrading software tools, and installing small form-factor pluggable (SFP) modules and redundant network access. This resulted in a replication of more than 150 signals in the cloud. As part of VELP's traffic balance strategy, some data streams were moved to a separate Virtual LAN (VLAN). As a result of segregation, highly critical protection components, which respond to grid abnormal conditions in milliseconds, can now be communicated reliably.

1.4 VELP’s Cybersecurity Architecture

- Cybersecurity Architecture [5]: Several ICS cybersecurity standards and guidelines are followed by VELP, including NIST SP800-115, IEC 62443, and ISO 31000, which represent risk management. In addition to keeping the platform cybersecure, the VELP cybersecurity system supports studies regarding ICS cybersecurity, protocol-based attacks, intrusion detection, and threat detection for users and trainees. By utilizing advanced cybersecurity tools and technologies, VELP has been designed in a way to provide users with flexible remote access to cybersecurity tools and systems for training purposes. It should be noted that the trainee's access is limited because not all users should have access to specific parts of the platform where commands or configurations can be modified.
- The Claroty Solution: As part of the VELP, Claroty is used to protect operational technology assets and networks from internal and external cyberattacks and to fulfill audit and compliance requirements. Through either a passive or active method, it scans the network for security conditions and threats. This platform can also be used to train students.
- Other Cybersecurity Tools and Systems: VELP also enables cyberattack simulations and supports cyber threat studies using other tools, such as IEC 61850 Avenue, IEC 61850 Toolset, Goose Injector, SMV Injector, RTDS, and an AI-based Early Warning System (EWS).

2. Technical Evaluation of VELP's Applications for Critical Infrastructure Training Programs in Canada

The evaluation plan focused on two key categories:

- Platform Technical Evaluation: meaning how the developed experiential learning platform technically performs in the presence of various types of operating conditions.
- Remote Session Technical Evaluation: meaning how efficiently the platform performs during different types of online remote practices.

This section reviews how these evaluations were performed.

2.1 Learning-Focused Works

2.1.1 To what extent were the needs being addressed before project implementation?

The project could successfully fill the gap in the existence of a reliable, flexible, and cybersecure virtualized experiential learning platform for critical energy infrastructure research studies and remote vocational training at BCIT.

2.1.2 How project would work and address stated needs?

In terms of the process, the existing infrastructure including physical assets and systems was used as initial resources. Moreover, cloud-based applications, hardware-in-the-loop simulators and models, new firmware, modules, and hardware tools were used to deliver project outputs. In terms of the outcomes, as shown in Fig. 1.1, the main result of the successful delivery of this project is to implement and run an online experiential learning environment for specialized education that supports safe and cybersecure remote access, as well as providing such platforms with proper pedagogical models to facilitate experiential learning. This includes various levels of outcomes as follows:

- Individuals: BCIT students and trainees can now use VELP to gain hands-on experience remotely through the virtualization technologies provided. Trainees from other institutes and/or companies are able now to benefit from using this platform as well.
- Institutions: the outcome of the project could help Canadian academic institutions learn how such experiential learning platforms could change the way of teaching and training hands-on skills.
- Systems: in a broader scope, the developed VELP could be integrated with other existing platforms around Canada and/or the globe in the future to enhance experiential learning through various types of advanced virtualization and digital twinning tools and technologies.

2.1.3 What assumptions were initially made about the project to achieve its objectives?

This project needed to stay highly technical in order for the team to focus on specialized educational materials and developing a remote hands-on training platform for critical energy infrastructures and industrial control cybersecurity. That is why this project was exempted from the REB review.

2.1.4 What contextual factors were anticipated that might affect how the project is delivered?

There was no issue with contextual factors.

2.1.5 What has been tested in this project?

The following technical items have been successfully evaluated and tested in this project:

- Proper communication between different components and systems

- Data accuracy from physical assets to the cloud and vice-versa
- Data monitoring using cloud-based applications.
- Platform's technical performance
- VELP's reliability and availability
- Virtualization capability
- Flexibility of the platform
- Cybersecurity of the platform
- Remote access to VELP's systems

2.1.6 How was success initially articulated for this project?

In this project, the success has been defined as:

- Completing the development of a reliable, flexible, cybersecure, and fully functional virtualized experiential learning platform and making the platform ready for remote critical infrastructure-related activities such as vocational training, research, and skill development.
- Testing the developed VELP in the presence of various operating conditions including different online practices/course modules.

We could successfully reach the above targets within the project's pre-defined timeframes.

2.2 Theory of Change and Logic Model

According to the project's theory of change, remote hands-on training courses, experiential learning through virtualization technologies, and research on critical infrastructure and industrial control cybersecurity were the key aims of developing VELP. The VELP has been developed and configured successfully with the support of our industry partner, Siemens Canada, and all outputs (i.e., clusters) mentioned in the figure of Theory of Change (Fig. 2. 1) have been successfully completed. The outputs provide the outcomes that need to be evaluated technically in this project to ensure:

- Safe and cybersecure remote access to VELP
- Support online experiential learning, and
- Proper pedagogical models to be found to facilitate remote experiential learning

2.3 Evaluation Key Goals:

The key goals of the evaluation plan were to:

- Facilitate further improvements
- Generate and disseminate technical knowledge
- Support other Canadian academic/research institutes in terms of technical development of similar virtualized experiential learning platforms, and
- Report how the technical performance of such platforms can be evaluated and how similar steps can be taken to develop a remote experiential learning platform.

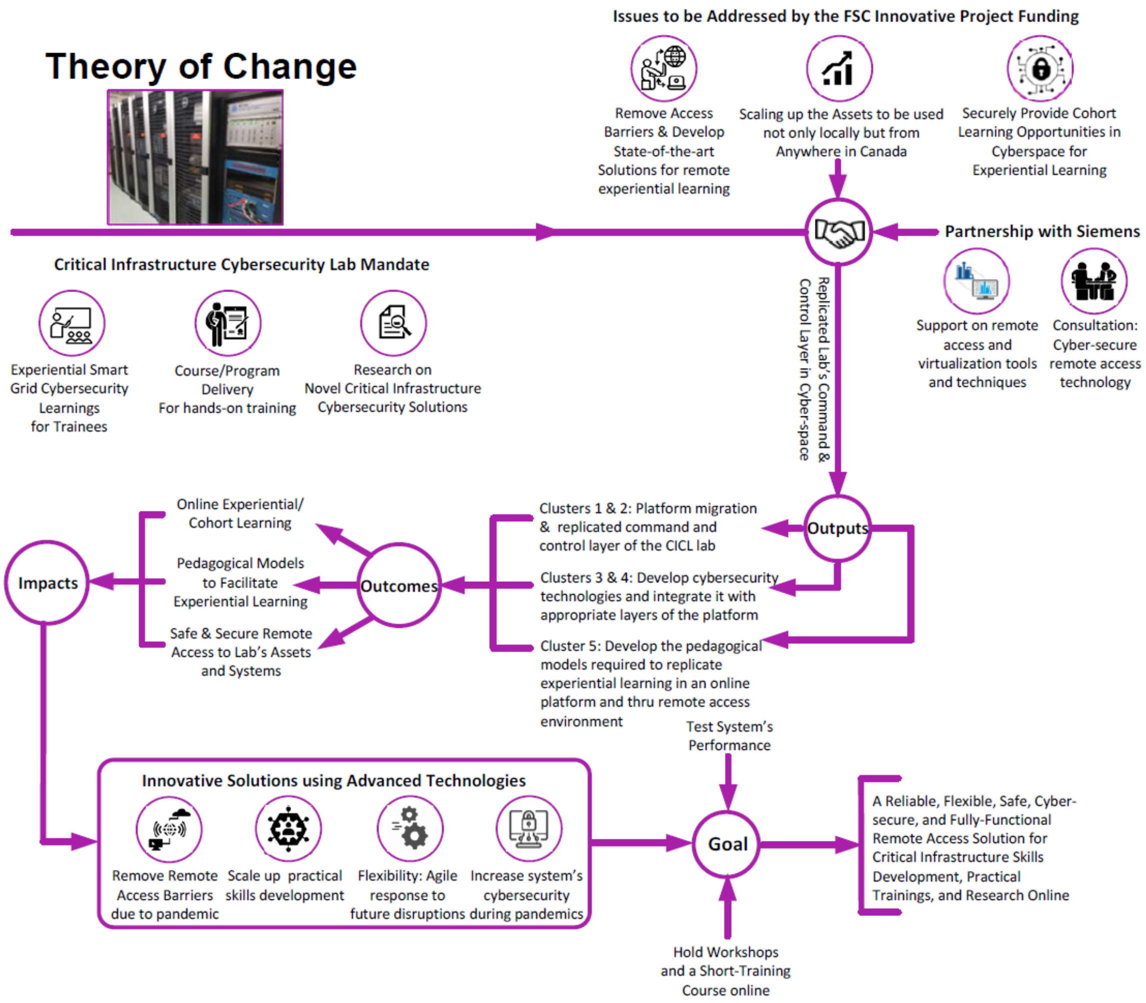
Theory of Change
Issues to be Addressed by the FSC Innovative Project Funding
Remove Access Barriers & Develop State-of-the-art Solutions for remote experiential learning
Scaling up the Assets to be used not only locally but from Anywhere in Canada
Securely Provide Cohort Learning Opportunities in Cyberspace for Experiential Learning
Partnership with Siemens
Support on remote access and virtualization tools and techniques
Consultation: Cyber-secure remote access technology
Critical Infrastructure Cybersecurity Lab Mandate
Experiential Smart Grid Cybersecurity Learnings for Trainees
Course/Program Delivery For hands-on training
Research on Novel Critical Infrastructure Cybersecurity Solutions
Replicated Lab's Command & Control Layer in Cyber-space
Outputs
Clusters 1 & 2: Platform migration & replicated command and control layer of the CICL lab
Clusters 3 & 4: Develop cybersecurity technologies and integrate it with appropriate layers of the platform
Cluster 5: Develop the pedagogical models required to replicate experiential learning in an online platform and thru remote access environment
Outcomes
Online Experiential/ Cohort Learning
Pedagogical Models to Facilitate Experiential Learning
Safe & Secure Remote Access to Lab's Assets and Systems
Impacts
Innovative Solutions using Advanced Technologies
Remove Remote Access Barriers due to pandemic
Scale up practical skills development
Flexibility: Agile response to future disruptions
Increase system's cybersecurity during pandemics
Test System's Performance
Goal
Hold Workshops and a Short-Training Course online
A Reliable, Flexible, Safe, Cyber-secure, and Fully-Functional Remote Access Solution for Critical Infrastructure Skills Development, Practical Trainings, and Research Online

Fig. 2. 1. Project's Theory of Change

2.4 Training Gaps/Needs

In VELP's training programs, trainees learn the fundamentals of critical energy infrastructures and their cybersecurity needs. Students are introduced to critical infrastructures and their cyber vulnerabilities. During training sessions, students learn how to perform risk and vulnerability assessments, develop cyber-architectures, and use advanced detection, mitigation, and restoration tools and technologies, all of which are necessary for performing cybersecurity practices in industries, utilities, and other sectors. After completing these training programs/modules, learners will achieve the following outcomes and competencies:

- Understand how different critical infrastructures work solely and together
- Learn the fundamentals of operational technology, industrial control systems, and critical infrastructure cybersecurity
- Designing proper cybersecurity architectures for critical infrastructures
- Accurately assessing risks and vulnerabilities
- Maintaining cyber security by utilizing proper threat detection solutions
- Proposing effective mitigation solutions for different infrastructures
- Become familiar with critical infrastructure cybersecurity planning (short-term and long-term)

- Learn about incident response methods and restoration techniques
- Learn how to keep Indigenous communities' critical infrastructures secure
- Keep knowledge current and updated to maintain important job skills

Furthermore, the proper implementation of automation systems at digital substations could have a substantial impact on the efficiency of power and energy grids. Today's electrical grids rely heavily on substations as the main hubs, the places where energy flows into and out of the grid. By automating substations with SAS, they can become faster, smarter, and can reduce carbon emissions and accommodate more renewable energy as well as comply with today's and tomorrow's energy needs. Energy transitions to net zero require new technologies to facilitate multidirectional energy flows and to enable grid systems to react faster to grid changes to keep electrical grids reliable and stable. It is possible to achieve this goal by implementing automation systems within our digital substations. To provide the workforce in this field with the hands-on skills necessary to implement Substation Automation Systems, and to support Clean-BC Roadmap to 2030 [6] key actions that contribute to cleaner industries/utilities, developing and delivering training programs/modules would be beneficial.

2.5 VELP’s Training Programs: Benefits to Canada

With the gaps listed in summary and the need for a reliable, flexible, and cybersecure virtualized experiential learning platform for critical infrastructure training, BCIT VELP could benefit a number of groups of Canadians, such as:

- A student from anywhere in Canada who is eager to learn about CI and CI cybersecurity.
- Scholars and researchers from academic and research institutes.
- Those who would like to attend professional development activities within the utility and industry sectors.
- Newcomers to Canada interested in learning about current CI tools and technologies.
- Indigenous communities: who would like to educate themselves, learn how to maximize the use of their systems, reduce GHG emissions, and reduce their dependence on diesel power.
- Regulatory and security agencies can use the system to model threat scenarios and consequences to help define regulation and cyber posture standards.
- Vendors can use the system to identify the readiness of new products and ensure that they do not inject new vulnerabilities.

Through VELP, learners will be able to work with advanced cybersecurity modeling and simulation tools. These training courses will provide substantial value to Canada and its various sectors, as learners can contribute to the cybersecurity aspects of these sectors. With the support of an industry partner, BCIT's SMART department is developing and delivering two micro-credentials. To avoid duplication and ensure alignment with learner needs, we also work with internal departments at BCIT, local hydro, and industries. In the near future, we plan to include and instruct other important critical infrastructures that have been ignored in our training programs, such as co-generation and water treatment facilities of Indigenous communities. By doing this, first nation communities could learn how to control their infrastructure themselves, which may reduce costs or could help them migrate from conventional systems to a modern automated system, which may reduce greenhouse gas emissions. Through VELP, training programs can now be delivered online. Throughout our institutional processes that align with post-secondary standards and policies, the plan is to periodically review and improve training programs to ensure value for learners. Through the use of advanced virtualization tools and technologies, VELP is able to provide a unique environment for innovative training programs that correspond to the needs of Canada's critical infrastructure.

2.6 Technical Validation/Evaluation Through Pilot Sessions - Results

Two pilot sessions with a limited number of students have been conducted by SMART to evaluate BCIT's virtualized experiential learning platform's applications for critical infrastructure training programs. Substation automation practices were covered in the first training session, and cybersecurity practices for critical infrastructure were covered in the second. To assess VELP's effectiveness and performance, the following tests were conducted before and during pilot sessions:

- Remote access/communication
- Normal operating use cases
- Communication signals
- Simultaneous multiple access
- Abnormal operating conditions

2.7 Pilot Session Validation Analysis

Following the two pilot sessions mentioned in the previous section, we asked trainees to respond to a technical survey. The results of the pilot sessions indicate that BCIT's virtualized experiential learning platform is able to provide trainees with a virtual learning environment for hands-on skill development. Here is a summary of the improvements that can be made to VELP's training modules and performance according to the survey:

- It might be overwhelming for some trainees to have so many tools at their disposal. It is best to provide trainees with adequate instruction and time to become familiar with the tools they will use in advance.
- In some training modules, group activities will be divided into teams using RTDS and NovaCor. To accommodate more groups, it would be better to provide more simulation racks in the future.
- It is easy to access, but a single sign-on system would be more helpful to trainees.
- A VELP could be integrated with other existing platforms/programs, such as Natural Resource Canada’s cybersecurity program, to enhance trainees' hands-on experience.

3. Project Partners - Experience

We had the pleasure of working with Future Skills Centre and Siemens Canada on this great project. This partnership was one of the best experiences our team had so far. In addition to being a partner with FSC and Siemens Canada, we have worked with RTDS Technologies on providing adequate hardware-in-the-loop real-time simulations for different critical energy infrastructure training/studies. We are thankful for their great support.

3.1 Partnership with Future Skills Centre

Partnering with Future Skills Centre on this fruitful project was a true pleasure for us. The experience of working with FSC and Siemens Canada was amazing and productive for all teams involved. The FSC team helped our team receive the knowledge required for managing projects, and running projects considering equity, diversion, and inclusion and provided us with the knowledge required for reporting. Through the FSC's webinars and events, our team was able to gain a deeper understanding of the net-zero economy and how to fill skill gaps in Canada's critical infrastructure and find innovative solutions. We were also continuously supported by the FSC team during the first and second years of the project. If we had any questions about project budget cost categories or line items or wanted to request a minor change to our plan, the FSC team promptly responded to our request and answered our questions.

Additionally, they assisted us in creating a technical evaluation plan and finding other institutions that may want to develop their own virtualization platforms in the near future. We really appreciate the collaboration and support from FSC, and we hope to have the opportunity to work with the FSC team on other projects in the future if possible.

3.2 Partnership with Siemens Canada

Siemens Canada immensely supported this project, from the beginning to the end, as an industrial partner. The outcomes of the technical evaluation could show how Siemens Canada could contribute to the development of such platforms for experiential learning across Canada. During the first year of the project, Siemens Canada helped us with the project's preliminary study, design, data collection, and tests and provided us with professional services. They also provided the project with a great amount of in-kind contribution in the first year of the project. This was to work with us on preliminary studies, design, consultations, review of technical documents, and other services. In the second year of the project, Siemens Canada provided professional services for developing the cybersecurity platform and integrating it with the main platform. They also provided us with an in-kind contribution mainly for supporting us in developing course modules and use cases, operation, and maintenance of the developed VELP, technical evaluation, technical tests, and troubleshooting the platform and its cloud applications. All stakeholders of this project worked together to determine the data collection procedure, facilitate technical data/signal collection, prepare technical evaluation questions and methods, and finalize project activities. Moreover, the stakeholders worked together in finalizing the technical evaluation results mentioned in this report and had workgroup meetings to review training/course materials integrated with BCIT's learning management system and find proper pedagogies for each.

In summary, the partnership with Future Skills Centre and Siemens Canada was a fantastic experience and it led to a project with fruitful outcomes, mentioned in the next chapter, that support Canadians in terms of experiential learning and utilization of virtualization technologies for vocational training.

4. Knowledge Mobilization

In this project, knowledge mobilization had been defined as one of the most important objectives. As such, our team had a comprehensive plan to disseminate knowledge gained from the technical outcomes of this project. As a part of the evaluation plan, the following table presents knowledge mobilization activities done by our team to articulate how project outcomes can be used by other stakeholders around Canada to develop an effective virtual version of their critical infrastructure for different purposes such as vocational training, research, monitoring, operating, control, conduct maintenance, and evaluate cybersecurity.

Table. 4.1. Events Conducted/Attended

Knowledge Mobilization Activities	**Description:**	**Date**
Lecture Session-1	A full lecture session was held for BCIT School of Energy students to introduce VELP.	May 12, 2022
Lecture Session-2	Another full lecture session was held for BCIT School of Energy students to show VELP's features and functionalities.	May 13, 2022
CEATI Workshop	Presented project outcomes, share knowledge gained, and receive feedback.	May 17, 2022
FSC Event: Skills for a Net-Zero Economy	Attended the event to share knowledge gained in the project and look for possible collaborations.	Oct. 25, 2022
CIGRE Canada Conference	Attended the conference to present a recently accepted paper [7] about the outcomes of the project. Shared knowledge and experience with other experts in the field and receive feedback.	Nov. 1-2, 2022
Webinar-1	Introduced VELP to the IEEE Smart Grid Society, and share knowledge gained from implementing the project.	Nov. 15, 2022
Seminar	Explained VELP's operating scenarios to potential trainees.	Nov. 16, 2022
IEEE EPEC 2022 Conference	A technical paper has been accepted, presented, and published [8] which shares virtualization approaches and lessons learned from the implementation phase of the project.	Dec. 5-7, 2022
IEEE ICIR 2022 Conference	Attended the conference and presented a recently accepted and published paper [5] about project implementation results. Shared knowledge and experience with other scholars in the field and received technical feedback.	Dec. 14-16, 2022
Workshop	Provided attendees with more details about virtualization and automation in modern digital substations	March 2, 2023
Webinar-2	FSC Project Talk Session. Shared knowledge and experience gained from the project with other experts in the field with FSC.	November 15, 2022
Training Session	Provided attendees with technical details of the developed VELP in cyberattack scenarios. Run use cases for remote hands-on practices.	March 3, 2023
Webinar-3	Provided attendees with technical details of the developed VELP. Shared lessons learned from the project with other experts in the field.	February 22, 2023

In addition to the above table, our team attended several events to gain the required knowledge for the project, introduce the developed VELP to experts in the field, share the outcomes of the project, and receive feedback. Table 4.2 shows some of the events our team members attended:

Table. 4.2. Activities and Event Participations

Knowledge Mobilization Activities	Date	Knowledge Mobilization Activities	Date
Generate 2022 Conference	May 2-3, 2022	FSC's Skills for a Net Zero Economy Event	October 25, 2022
Training Session	February 2022	FSC Webinars	2021-2023
VIPSS Summit	Feb. 22 – Feb. 24, 2023	FSC CoP	2022-2023
Training Session	February 22, 2023	Technical Focus Group Meetings	Jan.-March 2023
NRCan – CYDEF Training Session	Feb. 22 – Feb. 24, 2023	User involvement during tests	Aug. 2022-March 2023
Future Skills Summit	Feb. 22 – Feb. 24, 2022	Discussion meetings of stakeholders	April 2021-March 2023

The following table (Table 4.3) shows technical papers, posters, and abstracts that have been submitted to international conferences. Students could also present their work virtually at this conference. In addition to the above works, we are so excited to share that our "Fundamentals of Substation Automation Systems" micro-credential proposal has been accepted by the Ministry of Post Secondary & Future Skills (March 21, 2023). This micro-credential uses VELP developed in this project to provide trainees with hands-on skills in substation automation systems. The plan is to deliver this micro-credential starting September 2023.

Table 4.3. Technical papers, posters, and abstracts submitted.

Event Name	Paper Title	Date	Status
2022 CIGRE Canada Conference – Calgary, Canada [7] (in collaboration with Siemens Canada)	Virtualization of the Experiential Learning Platform for Critical Energy Infrastructure using Digital Twin Technology and Cloud-based Applications	Nov. 1-2, 2022	Accepted/Presented
IEEE Electrical Power and Energy Conference (EPEC 2022) – Virtual [8]	Virtualized Experiential Learning Platform for Substation Automation and Industrial Control Cybersecurity	Dec. 5-7, 2022	Accepted/Presented
IEEE International Conference on Intelligence Reality (ICIR 2022) – Virtual [5]	Virtualized Experiential Learning Platform (VELP) for Smart Grids and Operational Technology Cybersecurity	Dec. 14-16, 2022	Accepted/Presented
IEEE International Conference on Intelligence Reality (ICIR 2022) - Virtual	Modern Pedagogical Models for Virtualization Technology-based Experiential Learning Platforms	Dec. 14-16, 2022	Accepted/Presented
IEEE International Conference on Intelligence Reality (ICIR 2022) - Virtual	Cybersecurity Practices and Solutions for Virtualized Experiential Learning Platforms	Dec. 14-16, 2022	Accepted/Presented
ICS Security Symposium - Virtual	Cybersecurity of Communication Protocols in Smart Microgrids and Advanced Digital Substations	April 27, 2023	Accepted/Presented
2023 CIGRE Canada Conference – Vancouver, Canada [9] (in collaboration with Siemens Canada)	Virtualization Technology Applications in Advanced Digital Substations	September 25-28, 2023	Accepted/Presented
2023 CIGRE Canada Conference – Vancouver, Canada [10] (in collaboration with Subnet Inc.)	Application of Cyber Security Frameworks for Power System Cyber Threat Modeling and Training using Digital Twins	September 25-28, 2023	Accepted/Presented
Whitepaper	Modern Pedagogical Models for Virtualized Experiential Learning Platforms for Critical Energy Infrastructure Training	April-May 2023	Will be uploaded to BCIT Website

5. Final Discussions, Conclusions, and Future Works

BCIT considers this project to be a great success and a significant contribution to the state of the art. This section briefly explains some of the future potentials of using VELP. A few lessons learned are also outlined.

6.1 Expansion

The project has great potential to be expanded to support groups and communities that are interested in building a similar platform or working with BCIT's VELP for remote experiential learning. Moreover, other training modules, courses, and programs can be developed utilizing tools, components, and systems that have been gathered in a unique environment throughout this project. The VELP team is already making great progress by developing and delivering two new micro-credentials from the outcomes of this project. Further expansion is being planned. This project created an important body of knowledge on how to create efficient and cybersecure virtual experiential learning opportunities for trainees, in the wake of social or physical restrictions imposed by abnormal events. An offshoot of this experience is useful in helping organizations plan business continuity when physical access to assets is not possible or restricted. Although this project dealt with a specific domain of critical energy infrastructure, the body of knowledge it created would benefit other domains as well. The project established a repeatable and reusable process for other organizations to migrate the command-and-control layers of their physical assets to cyberspace and provide safe and secure access for trainees for "experiential learning by doing".

6.2 Adoption

Due to the nature of the project, which was highly technical, one of our mandates was to ensure that the platform is fully operational, reliable, and secure first. This has been achieved during the last two quarters of the project. As such, we highly believe that the created body of knowledge could be correspondingly utilized in other critical infrastructure domains such as hospitals, military campuses, commercial facilities, water and wastewater systems, and other power systems domains such as distribution networks and electric vehicle charging stations. VELP is open to academic students, researchers, industrial experts, underserved communities, recent immigrants, first nations, and remote communities, who would like to perform novel research, test, or get trained on critical energy infrastructure and its cybersecurity.

We believe that other organizations can significantly benefit from the outcomes of this project as well as the technical evaluation results. The project outcomes provide other organizations with the knowledge required to build such platforms for delivering remote hands-on training programs. The project works/steps related to the approaches/indices such as integration tests, technical data, observation methods, virtualization steps, and operating tests are useful for other organizations who are on the same journey. These works/steps can be found in our published papers. The project also delivered proper pedagogical models that are reusable by other organizations. Please see the technical papers that have been published by our team so far which are mentioned in the previous chapter of this report (chapter 5).

6.3 Partnership

It was BCIT's pleasure to be in partner with Future Skills Centre as well as Siemens Canada in this project. The platform has the potential to attract additional partnerships and collaborators from other organizations such as academic institutions, utilities, and industrial companies after project completion in the near future. We began forming new partnerships during the last quarter of our project. We are in the process of finalizing our partnership with an industry leader in operational technology cybersecurity solutions and services. Our team presented a technical paper at CIGRE Canada 2023 on the outcomes of this collaboration [10]. Moreover, we are happy to share a recent partnership with Edge Tune Power Inc company on microgrid digital twin modeling and real-time simulation.

6.4 Lessons Learned (What Worked? What Not?)

Note 1: This section summarizes lessons learned from the project's final activity report.

Note 2: The results and the learning outcomes that are explained in this section were published in technical papers mentioned in section 5 of this report.

In this project, we gained valuable insights into planning, designing, and developing virtualized experiential learning platforms. We found that this approach is effective for studying critical infrastructure. We learned the necessary steps for creating such platforms and for digitally twinning existing systems. Our team discovered how to establish reliable communication between different assets and systems in both physical and cyberspace using appropriate protocols. We also learned to verify the accuracy of data transmission between physical assets and the cloud by comparing digital twin data. Additionally, we mastered the integration of various virtualization tools and technologies into these platforms and tested their technical performance.

Furthermore, we understood the importance of making experiential learning platforms flexible to cater to the diverse training needs of adult learners. We also acquired knowledge in cybersecurity measures to maintain the security of these platforms. Moreover, we developed methods for secure access to digital twins and cyber-physical systems. Our collaboration with Siemens Canada and the Future Skills Centre was highly successful, and we appreciate their continuous support. We successfully achieved all our technical objectives and targets for the project. Overall, this project has equipped us with valuable knowledge that can be shared across Canada and applied to other domains. It was a rewarding experience collaborating with our partners, and we look forward to future opportunities for innovation and growth.

We successfully replicated the command-and-control layer in cyberspace. Multiple cloud-based applications like digital twins, dashboards, and navigators were successfully provided to trainees remotely. The cybersecurity interface was successfully developed and integrated with the entire platform. As included in the work plan, we integrated and tested the new experiential learning platform and conducted pilot training sessions. Our platform and training content were successfully integrated with BCIT's learning management system. Last but not least, we studied pedagogies that would facilitate the development of training modules and practices for adult/professional students. We had the opportunity to share the knowledge gained from this project with others. Four webinars/seminars, two pilot sessions, and two training/workshop sessions were successfully conducted. Our work was presented/published at three international conferences. Additionally, our students presented two posters. We could also submit three technical abstracts to great technical events. A total of six students were supervised and over 250 people participated in our knowledge mobilization activities during the course of the project.

Despite our achievements, we encountered several challenges during the project:

- Timely Design, Integration, and Testing**:** The design phase took longer than expected due to the complexity of the platform. Integration of systems with different technical features also proved time-consuming. Additional research assistant hours were allocated to address testing and verification delays.

- Pace of Development: Advanced virtualization technologies helped minimize data delays, but collaboration with BCIT's IT services was crucial to ensure a reliable communication network.
- Semiconductor/Chip Shortages: Equipment delivery faced delays due to chip shortages. Siemens Canada helped adjust technical plans and ensured timely delivery.
- Lack of Knowledge on Security Integration: Integrating with Security Assertion Markup Language (SAML) posed challenges. Support from Siemens Canada aided in filling knowledge gaps and validating cybersecurity integration.
- Integration with BCIT's Energy Management System (EMS): Integrating BCIT's EMS with the virtualized learning platform was identified as beneficial. With assistance from the Future Skills Centre, progress was made on this integration.

To address similar challenges, we offer the following advice:

- Invest Time in Design and Collaboration: Engage in thorough discussions with industry partners during the design phase.
- Prioritize Flexibility, Reliability, and Cybersecurity: Ensure that flexibility is considered alongside reliability and cybersecurity.
- Plan Integration Carefully: Comprehensive planning and consideration of future expansions are crucial for successful integration.
- Allocate Sufficient Time for Testing: Adequate time for testing, troubleshooting, and verification is essential.
- Adaptation and Open-Source Integration: Consider integrating with open-source tools to enhance compatibility with other platforms and provide advanced training opportunities.

This report highlighted the growing interest among industrial companies, enterprises, and utilities in retraining their staff with advanced technologies, such as IoT, AI, and Virtualization, to address skill gaps in Industry 4 & 5. Canada's increasing demand for clean energy jobs, estimated to reach 639,200 by 2030, underscores the need for policymakers and funders to support training opportunities, particularly through advanced solutions like experiential learning in clean energy. Developing virtualized experiential learning platforms for various critical infrastructures can engage trainees nationwide. These platforms enable a deeper understanding of infrastructure, leading to quicker and more accurate decision-making. Digital Twin projects provide accurate real-time models of systems, aiding in monitoring, tracking, and problem anticipation and mitigation, particularly during abnormal or catastrophic events. Virtualizing infrastructures enhances communication, reconfiguration, maintenance, validation, and operation of critical infrastructure. Proper funding and policies to support such projects can facilitate Canada's transition to a net-zero economy and bolster its cybersecurity posture.

6.5 Benchmarking Summary

The benchmarking results have been shared through published papers at the CIGRE Canada conference, IEEE electrical power and energy conference, and the international conference on intelligence reality. By comparing the features and functionality of the above platforms, it can be concluded that only a few studies have been conducted on the design and development of a reliable and secure experiential learning platform for critical energy infrastructures for remote hands-on training purposes. VELP uses advanced virtualization technologies such as digital twins, cloud-based monitoring, and optimization applications to provide its users with remote vocational training. The greater impact of this approach would be that such training could be offered to individuals and communities across Canada and the globe. Table 6.1 compares some of the features of the developed VELP with common/existing experiential learning platforms.

Table. 6.1. Developed VELP Features compared with other platforms.

No.	Feature	Comparison
1	Multi-user remote access	From the literature, it has been found that there are not many experiential learning platforms available with multi-user remote access capability. Many remote access technologies connect third parties to real physical systems for evaluation, data collection, scheduled maintenance, tests, and troubleshooting purposes. The developed VELP is able to provide trainees with remote access to the digital twin models of critical energy infrastructure such as microgrids and substations. Moreover, trainees have access to cybersecurity tools and cloud applications that are used for hands-on training purposes.
2	Using advanced virtualization technologies	Not so many platforms use advanced virtualization technologies. Our developed VELP not only uses advanced virtualization technologies such as digital twins, cloud navigator, and dashboard, but it uses advanced continuous threat detection systems and enterprise management consoles for cybersecurity studies. Moreover, VELP uses 3D models of infrastructures under study to provide trainees with 3D visualization of real-field components.
3	Using Cloud for training purposes	Although some platforms/energy infrastructures use the cloud for monitoring and data analysis purposes, we could not find many educational platforms that use cloud applications for vocational training. VELP uses different substations and microgrid cloud-based applications to provide trainees with such hands-on training.
4	Keep the platform's cybersecurity in consideration	Utilities and industrial companies have recently become more vigilant regarding cyber vulnerabilities and many of them have sorts of cybersecurity plans to comply with the standards and frameworks such as NIST. However, we could only find platforms with minimum cybersecurity tools (not advanced) for training purposes. VELP uses advanced cybersecurity tools to not only keep the platform cybersecure against cyberattacks but to provide an environment for trainees to learn more about such advanced cybersecurity solutions/technologies.
5	Cybersecurity tools for remote training	As mentioned in 4, VELP uses advanced cybersecurity tools for remote hands-on training on advanced cybersecurity solutions for critical energy infrastructures.
6	Flexible virtualized experiential learning platform	For remote vocational training, it is essential to develop a flexible platform where trainees be able to work with different types of tools and technologies easily. Moreover, the platform should be flexible to a certain degree to support future expansion. Our developed VELP is a flexible platform that gathered/integrated various tools and technologies under the same roof to support different remote hands-on training programs. There are not many platforms available with such flexibility degree.
7	Reliable virtualized experiential learning platform	Experiential learning platforms need to be reliable, meaning that they need to operate with minimum failures. During this project, we tested VELP under different types of operating scenarios and investigated the failure rates of different tools and systems. From the outcome of these tests, we can say that the final version of VELP is a reliable, secure, and available experiential learning platform.
8	Support various types of critical energy infrastructure models	There are not many experiential learning platforms available that are able to support various types of operating scenarios and critical infrastructure models. The developed platform in this project is able to support different critical energy infrastructure models such as substations, different microgrids, power distribution networks, etc.
9	Support various types of operating scenarios for training purposes	VELP models can run in different operating conditions (e.g., the normal, line-to-ground faults, line-to-line faults, breaker failure, cyberattacks, etc.) that can be used in different training modules.
10	Integrate various tools and technologies for hands-on training	There are not many experiential learning platforms that could integrate various tools and technologies such as virtualization, simulation, digital twinning, and real-time simulation that are useful for remote hands-on training. Thanks to this project, the developed VELP could integrate and utilize several different tools and technologies such as digital twins, real-time simulation, 3D visualization, cloud applications for substation and smart microgrid studies, and cybersecurity solutions such as threat detection and enterprise management.

6.6 Next Steps/Future Works

This project opened a plethora of possibilities that are relevant and key to the critical infrastructure industry. With additional funding, BCIT will be able to undertake expansions to this platform and adaptation to other critical infrastructure. Examples include:

- SCADA-driven attacks on water and utility infrastructure
- A virtual table-top exercise to stress-test a utility cyber posture
- Implementation of industry-specific regulatory/mandatory compliance requirements such as NERC CIP
- Targeted micro-credentials for specific attack vectors such as:
    - Microgrid cybersecurity
    - Hijack of specific protection devices
    - Disabling control systems for low-impact systems such as EV charging stations, smart meters, and telecom systems

BCIT would be willing to provide more details and/or a proposal on any of the above areas in the near future.

As an extension phase, the project can empower audiences and stakeholders, especially those in remote communities, industry professionals, and newcomers facing skill demands in transitioning to a net-zero economy through the following success metrics:

1. Developing cost-effective and accessible training plans for community members, newcomers, and industry workers, quantifying benefits of BCIT's digital twin platform by:
    a. Comparing the developed platform with market alternatives and examining integration within industry-relevant platforms and training programs; and
    b. Evaluating platform’s benefits for community members facing access-related barriers.
2. Establishing remote flexible experiential learning environments using BCIT’s digital twin catering to industries, newcomers, and remote communities, enhancing hands-on training and knowledge dissemination capabilities
3. Conducting broad outreach and targeted marketing:
    a. Targeted outreach to one community as an example of contextualization for community needs.
    b. Canadian utility/industry organizations
4. Expanding knowledge mobilization efforts; and
5. Extend Evaluation studies to measure the project’s long-term outcomes and impacts on the target audience.

References

[1] Critical Infrastructure Cybersecurity Lab (CICL), [Online]: https://bcit.ca/smart-cicl

[2] Virtualization of Experiential Learning Platforms and their Pedagogical Models, [Online]: https://fsc-ccf.ca/projects/virtual-learning-infrastructure-sector/

[3] BCIT's Virtualized Experiential Learning Platform (VELP), [Online]: https://bcit.ca/smart-velp

[4] M. Shariat-Zadeh, M. Manbachi, A. Gomez, and H. Farhangi, "Virtualization of the Experiential Learning Platform for Operation and Maintenance of Smart Microgrid Applications in Remote and Rural Communities in Canada", CIGRE-484, CIGRE Canada Conference, Calgary, Nov. 2022.

[5] M. Manbachi, M. Hammami, "Virtualized Experiential Learning Platform (VELP) for Smart Grids and Operational Technology Cybersecurity", IEEE International Conference on Intelligence Reality, Dec. 2022.

[6] Roadmap to 2030, CleanBC, [Online]: https://www2.gov.bc.ca/assets/gov/environment/climate-change/action/cleanbc/cleanbc_roadmap_2030.pdf

[7] M. Manbachi, M. Shariat-Zadeh, I. Letvenchuck, and H. Farhangi, Virtualization of the Experiential Learning Platform for Critical Energy Infrastructure using Digital Twin Technology and Cloud-based Applications, CIGRE 481, CIGRE Canada Conference, Calgary, Nov. 2022.

[8] M. Manbachi, J. Nayak, M. Hammami, A. G. Bucio, "Virtualized Experiential Learning Platform for Substation Automation and Industrial Control Cybersecurity", IEEE Electrical Power and Energy Conference, December 2022.

[9] M. Manachi, I. Letvenchuck, I. Ahmed, K. Mohammed, V. Vankayala, "Virtualization Technology Applications in Advanced Digital Substations", CIGRE Canada Conference & Exhibition, CIGRE-600, Vancouver, BC, Canada, September 2023.

[10] K. Stich, M. Manbachi, J. Nayak and V. Vankayala, "Analysis of a Digital Twin Model Power System Cyber-Attack to Develop a NIST Cybersecurity Framework Control Profile," CIGRE Canada Conference & Exhibition, CIGRE-583, Vancouver, BC, Canada, September 2023.