VOL 1, ISSUE 14 **DECEMBER 2024**

IR³ FEATURE ARTICLES

2 Editorial Corner

5 Virtualized Experiential Learning Platform for Critical Infrastructure Cybersecurity Laboratory
Dr. Moein Manbachi, Minoo Shariat-Zadeh, Jay Nayak, Mohamed Hammami, and Dr. Vidya Vankayala

14 Teaching hands-on cyber incident response for SCADA Network
Dr. Antoine Lemay, Michael Noory, Dr. Felix Kwamena, Andrew Lackey.

23 Short Review of Machine and Deep learning Advancements in Wildfire Management
Aziz Al-Najjar, Dr. Marzieh Amini, Dr. James Green, Dr. Felix Kwamena

32 May 2024 solar storm observed by Health Canada's environmental radiation monitoring detectors
Tamara R. Koletic

39 Resilience in Leadership: Personal and Organizational Requirements and Effects of Building Resiliency
Valerie A.R. Keyes

47 Literature Corner
Intended to provide readers with articles and sources on topics of professional interest.
Dr. Felix Kwamena
Fac. of Eng. & Design, Carleton University

49 Calendar

Editorial Corner

Dr. Robyn Fiori

About the Editor

Dr. Robyn Fiori is a research scientist for the Canadian Hazards Information Service of Natural Resources Canada specializing in space weather. Her research is applied to the development and improvement of space weather tools and forecasts to be used by operators of critical infrastructures and technologies in Canada. Dr. Fiori's research has been published in numerous peer reviewed scientific journals, including the Journal of Geophysical Research, the Journal of Atmospheric and Solar-Terrestrial Physics, and Space Weather. Dr. Fiori received her B.Sc., M.Sc., and Ph.D., from the University of Saskatchewan, Department of Physics and Engineering Physics while studying in the Institute of Space and Atmospheric Studies. She can be reached at robyn.fiori@canada.ca.

This Issue

This five-article IR^3 Issue 14 covers a wide range of topics.

Recognizing the current hybrid work environment the Issue starts with the British Columbia Institute of Technology article on virtualized experiential learning platform that can be used for remote learning. Recent industrial expansion is supported by the rapid emergence of technologies such as IoT, cloud-based systems, machine learning, and Industry 5.0 innovations like virtualization and cognitive systems. These expansions have also added complexity and additional cyber vulnerabilities. Industrial sectors, enterprises, and utilities are under significant pressure to leverage these new technologies, while also preserving and protecting their cyber defenses. The utility sector faces critical shortage of skills and trained personnel and needed to either retrain their current workforce with these advanced technologies or hire experts from other fields to provide on-the-job hands-on training to bridge skills gaps. This paper describes BCIT's Virtualized Experiential Learning Platform which offers a robust hands-on environment for Canadians to train, upskill, or gain insights into critical energy infrastructure cybersecurity, and review its features and functionalities. The paper also identifies future work needed to keep up with the increasing demand for critical energy infrastructure cybersecurity training including the addition of more digital twins for specialized training areas such as EV charging infrastructure cybersecurity, Advanced Metering Infrastructure (AMI) and smart metering, IIoT, Virtual Power Plant (VPP), and advanced studies on Resilient Energy Systems. This expansion will enhance VELP's ability to provide comprehensive and practical cybersecurity training in critical energy sectors; as well as supporting larger inter-provincial energy system interfaces and operation.

With the increase of cyber incidents affecting critical infrastructure (CI) operations, there is a growing need to develop cyber security skills in the CI workforce. However, because industrial control systems (ICS) are Cyber-Physical System (CPS) operating business critical infrastructure, opportunity to develop hands-on experience is limited, especially with regards to cyber-attacks. Dr. Antione Lemay et. el. describes the use of a virtualized cluster replicating a SCADA network, to provide an environment where cyber-attacks could be safely run, and operational impacts (the physical component of the CPS) could be observed. Virtualized sandboxes are used to emulate the cyber components and simulate the physical components to show attack artefacts, optimize virtual machines to enable scaling to a classroom level, and leverage the shared hosting to facilitate interactions with the trainees in a fully remote setting.

The next two articles deal with climate change issues that have been widely reported in the media.

Recent wildfire seasons in Canada have reached unprecedented levels, burned millions of hectares, and threatened critical infrastructure. Aziz Najir's paper reviews the advancements in machine learning (ML) and deep learning (DL) technologies for wildfire management, emphasizing their transformative role across pre-fire, active-fire, and post-fire stages.

In pre-fire management, ML and computer vision techniques enhance fuel type classification, reducing fire hazards. For active-fire management, DL models improve real-time fire detection and mapping, enabling efficient resource allocation and community protection. Post-fire, ML and DL methods facilitate accurate burned area and fire severity mapping, supporting effective recovery efforts. By integrating these technologies, the paper highlights current capabilities and future directions in wildfire management, aiming to help bolster infrastructure resilience and safeguard human lives.

Tamara R. Koletic's article presents the work done by Health Canada using Fixed Point Surveillance (FPS) network to monitor real-time environmental radiation solar storm. Health Canada's Fixed-Point Surveillance (FPS) network is a nation-wide system of detectors developed to monitor both anthropogenic and natural radiation sources. The network consists of over eighty detectors, spanning from Resolute, NT in the north to Southern Ontario. A fleet of five RS252d detectors (sodium iodine spectrometers manufactured by Radiation Solutions Incorporate (RSI) were installed at the Natural Research Council of Canada (NRCan) near Anderson Road, Ottawa, in July 2023, to test a new gain stabilization algorithm. Due to the detectors' proximity, the combined signal of the fleet offered a better cosmic ray response with improved statistical uncertainty.

This report analyzes the response of these detectors to the strong solar flare activity and coronal mass ejections (CME) during May 7-14, 2024. CMEs are highly energetic particles/plasma and magnetic fields ejected from the sun during solar activity. Though cloud cover in Ottawa prevented residents from witnessing the brilliant display of aurora, the Anderson fleet captured the characteristic Forbush decrease caused by the solar storm. The rescaled cosmic radiation counts/s in the FPS network follow the same trends found in other radiation (i.e., muon and neutron) monitoring systems. The FPS responses match the onset and maximum disturbance times of the collocated NRCan's geomagnetic temporal profiles. This case study is another example that Health Canada's FPS network can be used for real-time space weather monitoring. And its data offers a different and complementary perspective on space weather events than NRCan's magnetic data, but with a comparable response profile.

Wrapping up Issue 14, is Valerie Keyes' article presenting a framework of resilience leadership.

Experience shows that resilience in leadership plays a major role in the attainment of personal, professional, and organisational goals as well as being an essential part of leadership responsibility and accountability. This paper examines the fundamental factors that build resilience at all levels of an organisation, from the individual to the leader, and thence to the whole organisation. It concludes with steps that will assist leaders to become more resilient, thereby building better and stronger organisations that can withstand challenges and adversities.

Next Issue

We invite authors to contribute articles for Issue 15 relating to their experience in the field of security and infrastructure resilience. Draft articles of 2500-4000 - words are requested by 28 **February 2025.** You may not have much time or experience in writing 'academic' articles, but IR^3's editorial board can provide guidance and help. Your experience is valuable and IR^3 provides an ideal environment for sharing it.

Virtualized Experiential Learning Platform for Critical Infrastructure Cybersecurity Laboratory

Dr. Moein Manbachi, Minoo Shariat-Zadeh, Jay Nayak, Mohamed Hammami, and Dr. Vidya Vankayala Smart Microgrid Applied Research Team (SMART), British Columbia Institute of Technology

Summary:

While the recent industrial expansion is supported by the rapid emergence of technologies such as IoT, cloud-based systems, machine learning, and Industry 5.0 innovations like virtualization and cognitive systems, they have also added complexity and additional cyber vulnerabilities. Industrial sectors, enterprises, and utilities are under significant pressure to leverage these new technologies, while also preserving and protecting their cyber defenses. The utility sector faces critical shortage of skills and trained personnel. They are needed to either retrain their current workforce with these advanced technologies or hire experts from other fields to provide on-the-job hands-on training to bridge skills gaps. Additionally, the demand for clean energy jobs in Canada is on the rise. In 2020, one in 26 Canadian workers held a green job, and the environmental sector workforce grew by five percent [1]. A 2021 report by Clean Energy Canada projects that by 2030, there will be 639,200 jobs in the clean energy sector [2]. This increases the critical need for academic and research institutions to address the skilled workforce shortage to support Canada's transition to a net-zero economy. Many experts recommend "Experiential learning" as an effective solution. This paper describes BCIT's Virtualized Experiential Learning Platform (VELP) [3] which offers a robust hands-on environment for Canadians aiming to train, upskill, or gain insights into critical energy infrastructure cybersecurity, and review its features and functionalities. This paper also identifies future work needed to keep up with the increasing demand for critical energy infrastructure cybersecurity training.

Background:

Virtually all aspects of modern life depend on energy infrastructure such as industry, commercial activity, homes, communities, telecommunications & broadcasting, disaster management, climate change, and agriculture. Over the past five years, the pandemic has drastically affected professional training programs that rely on experiential learning with actual physical platforms and on-site lab-based learning. These programs typically require interaction with real systems and physical assets, enabling trainees to engage with true-to-life environments and equipment. To overcome the challenges associated with limited access to in-person training and assets sharing the same physical location, BCIT's Smart Microgrid Applied Research Team (SMART) [4] has developed a Virtualized Experiential Learning Platform (VELP) in 2021-2022 and expanded its features in 2023 and 2024 to support remote hands-on training of various critical energy infrastructure. This platform uses digital twin models to support various real-field models in power and energy and allows instructional content to be accessed securely and remotely.

BCIT's Critical Infrastructure Cybersecurity Lab

BCIT's Critical Infrastructure Cybersecurity Laboratory (CICL) has been developed as a high-fidelity R&D platform for advancing research and educational initiatives in power systems, digital substations, smart microgrids, and critical infrastructure cybersecurity (Fig. 1) [5]. In 2020-2021, SMART secured funding from the Future Skills Centre (FSC) to create technology that digitally twins the "Command and Control" layer of physical assets in CICL, transitioning these control systems into cyberspace [6]. This led to the development of VELP

within CICL, equipped with advanced virtualization technologies such as cloud-based dashboards. VELP replicates the experience of working with real-world devices and systems, allowing trainees to remotely acquire a comparable level of understanding and expertise [7].

Fig. 1. BCIT's Critical Infrastructure Cybersecurity Lab (CICL)

To extend BCIT's VELP to a broader audience across Canada, the VELP customized its training content to provide hands-on, virtual training programs for Canadian professionals involved in energy systems such as substations and their automation systems, smart microgrids (both grid-connected and off-grid types), energy hubs, and related Operational Technology (OT) cybersecurity. VELP team also recognized the need for training new users or upskilling existing personnel in running remote or community energy systems where gaining this expertise is costly, inaccessible, or unavailable locally.

Introduction:

BCIT's Virtualized Experiential Learning Platform (VELP) uses a digital twin to closely mimic the operations of critical energy infrastructures like smart microgrids, substations, and other power grid components. The platform features two hardware-in-the-loop simulators that replicate energy system operational scenarios in real-time. It integrates with actual Intelligent Electronic Devices (IEDs) such as protection relays and merging units, which safeguard the system during abnormal events like line-to-ground or line-to-line faults. The digital twins of these protection devices are hosted in the cloud, enabling trainees to interact with these components. The microgrid model also links to a Distributed Energy Optimizer via an industrial microgrid controller, allowing trainees to manage real microgrid setups including grid-connected and off-grid scenarios remotely. For substation data monitoring and analysis, the platform utilizes SIPROTEC Dashboard and SICAM Navigator cloud applications. These applications allow trainees to monitor substation components such as circuit breakers and leverage near real-time and historical data to evaluate the performance of advanced digital substations. A visualization platform is also available, providing students with 3D visualizations of components of the energy infrastructure digital twin models. Fig. 2 illustrates the main architecture of BCIT's VELP. VELP has also integrated Claroty's xDome, a modular cybersecurity solution designed to enhance the security and resilience of critical infrastructures. xDome provides comprehensive visibility, robust protection, and efficient threat detection, supporting various asset discovery methods and integrating seamlessly with other security tools for vulnerability management and policy enforcement. It also offers secure remote access solutions, simplifying administration and ensuring compliance, which helps trainees comprehend and observe how cybersecurity mechanisms protect critical energy infrastructures against various cyber threats.

The core of VELP consists of a Real-time Digital Simulator (RTDS), a vital tool used for emulating power and energy grid models in real-time. It employs its software for modeling various electrical grids and components, enabling the simulation of different load and generation profiles and various power grid operating scenarios. RTDS supports comprehensive power system analysis including load flow, short circuit, fault tolerance, and more, while also allowing for the implementation of substation and microgrid control layers using protocols such as IEC 61850.

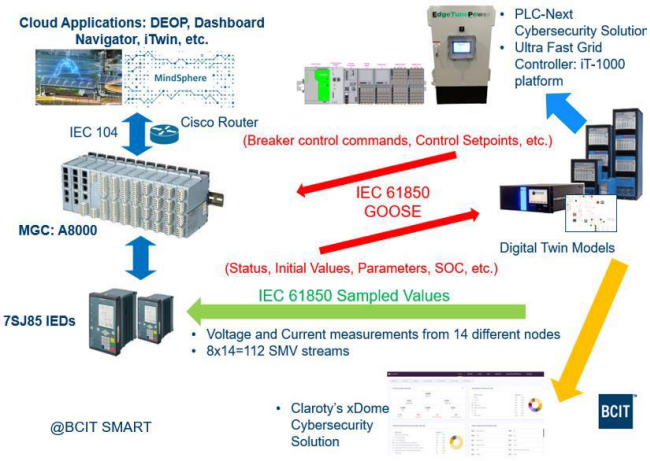

Fig. 2. BCIT's Virtualized Experiential Learning Platform (VELP)

VELP incorporates PB5 processing cards to simulate different grid models and execute power grid analyses such as load flow and switching transients, with trainees having access to two RTDS racks for simultaneous real-time model operations. NovaCor technology which represents the latest in simulation hardware used by RTDS is also used in VELP to significantly enhance computational and modeling capabilities with the potential to handle 90 nodes plus 180 load units. Presently, VELP operates with one NovaCor chassis equipped with more than three core licenses. Additionally, VELP integrates two Giga Transceiver Networking (GTNET) cards, supporting diverse industrial control protocols including Modbus, DNP 3, and IEC 61850. The VELP also utilizes RSCAD software across its various versions to model different energy infrastructures and critical components. For interfacing with real-world devices, the setup includes Giga Transceiver Digital Input (GTDI) and Giga Transceiver Digital Output (GTDO) cards, along with one Giga Transceiver Analog Output (GTAO) card for driving high voltages and currents needed for protection relays. Additionally, a Giga Transceiver Field Programmable Gate Array (GTFPGA) is used in VELP to mimic the Process Bus in real substations and support the publication of IEC 61850 sampled value streams from different grid segments.

Digital Substation Training using Digital Twins

VELP's real-time co-simulation digital twin platform simulates the operation of digital substation automation using protocols such as IEC 61850 GOOSE, Sampled Values (SV), Manufacturing Messaging Specification (MMS), DNP.3, and Modbus. Trainees can explore advanced solutions for automation, smart operation, and maintenance of Medium-Voltage (MV) substations using both basic and sophisticated substation models [8-9]. These models facilitate learning about various substation types as well as Substation Automation Systems and enable the investigation of the effects of cyberattacks on different substations and grid locations. The advanced model features a double-busbar topology integrated with fourteen different real-field intelligent electronic devices from various vendors, which communicate in an interoperable way using the IEC 61850 protocol [9]. In addition, VELP's digital twin model for substations facilitates hands-on training focused on protocol-based cyberattacks, modeling attack consequences on advanced substations using the IEC 61850 protocol and on conventional digital substations using DNP3 or Modbus. This model also supports training in cybersecure architecture, threat detection, and prevention strategies. The model incorporates sophisticated tools and technologies, including an industrial Human-Machine Interface (HMI) for monitoring and control alongside a digital twin HMI that operates concurrently for hands-on training on substation operating scenarios under normal, abnormal, and cyberattack conditions (Fig. 4). This setup includes a primary HMI PC and a backup PC, enabling trainees to learn how to receive data from various components, issue control commands to field devices, and monitor the entire critical energy infrastructure effectively. Additionally, the platform allows for the simultaneous operation of multiple models, offering collaborative and interactive learning opportunities for trainees.

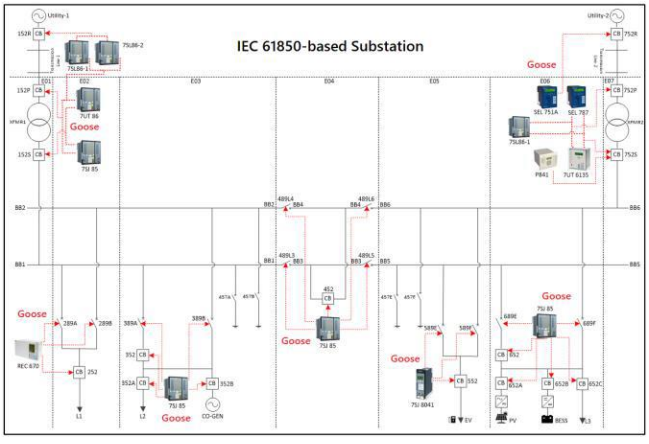

Fig. 3. Single line diagram of VELP's substation model

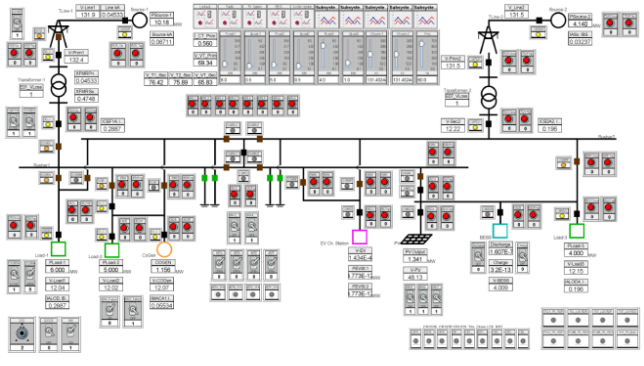

Fig. 4. Digital Twin of the Industry HMI in VELP

For hands-on learning, VELP also uses SIPROTEC Digital Twins in a cloud application to teach trainees about setting up and configuring protection schemes and integrating IEDs, enhancing their understanding of fault analysis and cybersecurity measures relevant to substation operations (Fig. 5). The platform is also equipped with cloud-based applications for substation data monitoring and analysis, such as the SIPROTEC Dashboard and SICAM Navigator (Fig. 6 and Fig. 7). These tools offer operational views of substations, enabling trainees to monitor device statuses, visualize grid models, and receive updates on abnormal operations directly through mobile and desktop interfaces, facilitating a comprehensive understanding of grid management and maintenance strategies.

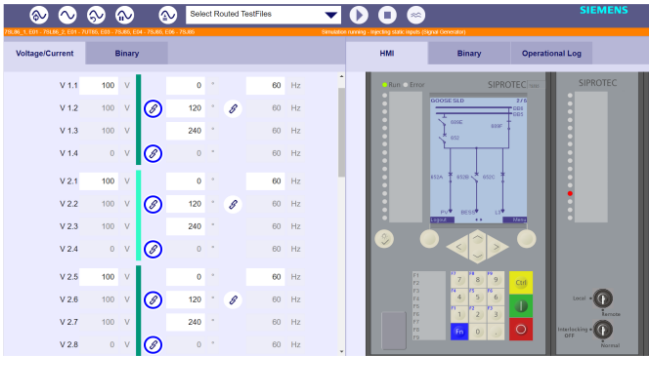

Fig. 5. VELP uses the SIPROTEC Digital Twin platform

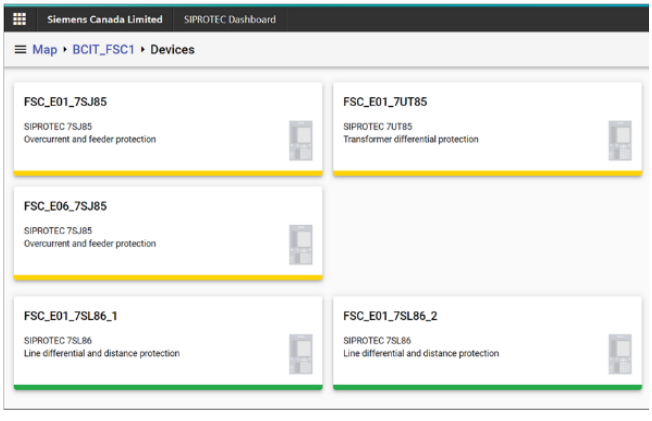

Fig. 6. VELP's SIPROTEC Dashboard platform

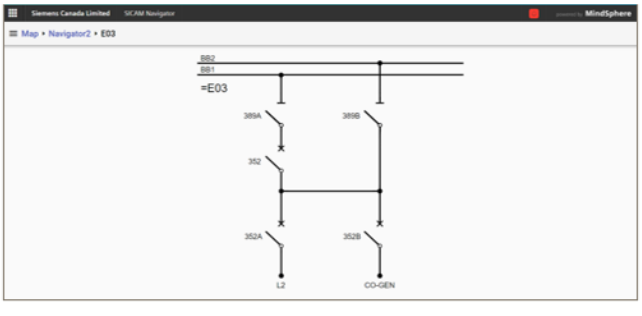

Fig. 7. VELP's SICAM Navigator cloud application

Smart Microgrid & Other Energy Infrastructure

BCIT SMART has transformed its smart microgrid training into a virtual hands-on environment through the use of advanced digital twin models of various types of smart microgrids by [10]:

- Digitally replicating the command-and-control layer of physical assets and transitioning this layer to cyberspace, enabling remote access to the training platform.
- Ensuring secure remote access for teams, facilitating secure collaborative work in cyberspace where team members can safely interact on various

operational aspects of the microgrid, sharing tasks, observations, and findings.

- Integrating virtualized physical assets with sophisticated educational materials provided through BCIT's Learning Management System (LMS) to support various learning formats including individual, cohort, and team-based approaches.

VELP's digital twin platform features three distinct smart microgrid types to simulate a range of microgrid topologies and operational scenarios:

- Conventional off-grid: This model covers remote systems in remote communities featuring diesel power plants and typical loads found in remote communities. It explores scenarios such as diesel reduction through increased use of renewable energy sources such as PVs and wind turbines, aimed at fulfilling the energy needs of remote communities.
- Off-grid Microgrid solutions: Suitable for remote communities, this model includes systems powered by a combination of Diesel Genset (either grid-forming or grid-following), Battery Energy Storage Systems (BESS), renewable energy sources (PV and wind turbines as grid-following resources), and typical community loads.
- Grid-tied Microgrid: This mimics the Energy OASIS Simulated Microgrid at BCIT, featuring grid sources, BESS, photovoltaic (PV) systems, wind turbines (WT), EV chargers, and typical loads, as well as islanding operation (Fig. 8).

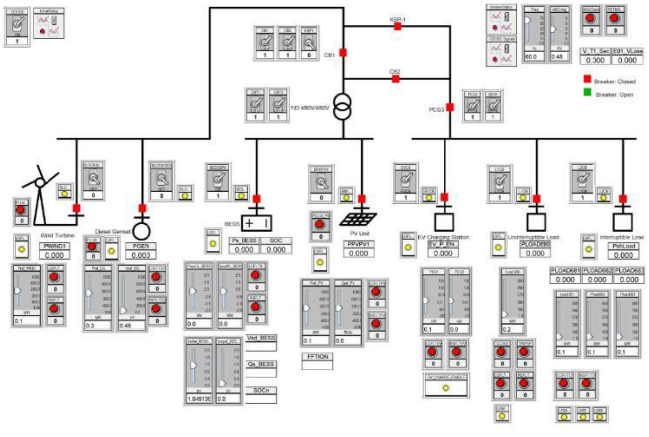

Fig. 8. VELP's digital twin model for a grid-connected microgrid

In brief, VELP could support different types of microgrid training, from operation and maintenance to architectural design, and from FEED study to cybersecurity studies for different target audiences such as remote communities, utilities, and industries. In addition to microgrids, VELP can virtualize other critical energy infrastructures or systems such as Energy Hubs, Battery Energy Storage Systems (BESS), single busbar substations, and Electric Vehicle (EV) charging infrastructure, supporting various training studies including cybersecurity, operation & maintenance, protection, and Fault Location, Isolation, and System Restoration (FLISR).

Critical Energy Infrastructure Cybersecurity Hands-on Training using VELP:

BCIT's SMART team has engineered a cyber-physical digital twin model within the VELP that integrates with previously described virtualized models for a comprehensive hands-on training experience in operational technology cybersecurity, focusing on power and energy grids. This model is specifically designed for conducting cyber vulnerability assessments on power grid protocols, using real-time simulations to expose vulnerabilities in protocols such as IEC 61850 (GOOSE and Sample Value) [9], DNP3, and Modbus [11]. It facilitates lab experiments where trainees can launch and analyze the effects of cyberattacks like Man-in-the-Middle (MITM) and Denial of Service (DoS), observing their impacts on power characteristics and control operations (Fig. 9) [11-12]. Such experiments demonstrate how these attacks could manipulate control actions, trigger protective mechanisms erroneously, or corrupt data communications, potentially leading to widespread failures in electrical grids. Through these simulations, trainees can deeply understand the ramifications of cyberattacks on communication protocols and the importance of robust cybersecurity measures in maintaining the stability and security of power systems. The insights gained from these assessments are crucial for developing effective cybersecure architectures, positioning them as vital defenses against cyber threats to critical energy infrastructures.

VELP also incorporates essential training resources for OT cybersecurity, including an educational game (Fig. 10) specifically designed for those new to the field.

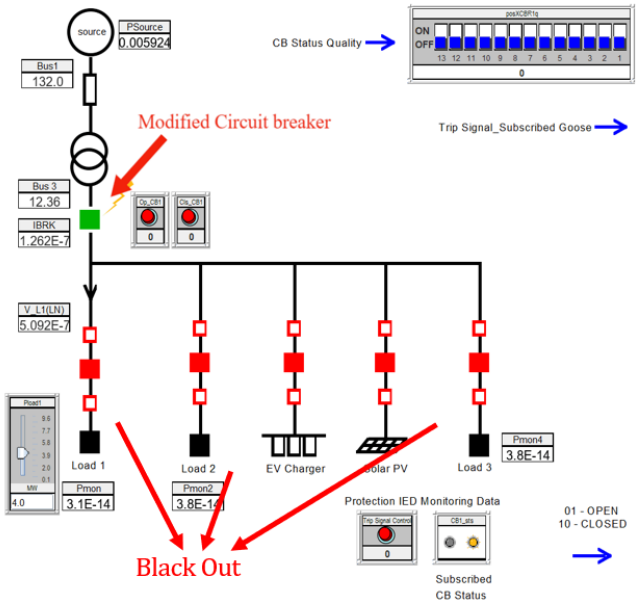

Fig. 9. Power system digital twin model for cyberattack consequence modeling practices.

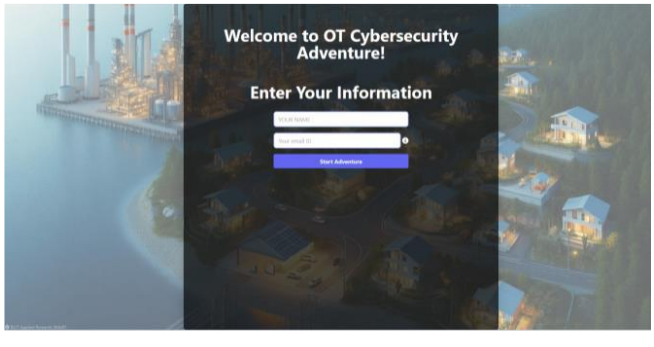

Fig. 10. VELP's OT Cybersecurity Game: OT Cybersecurity Adventure!

This game is intended to teach the fundamentals of OT cybersecurity in an interactive and engaging manner, making it accessible for beginners interested in learning about the security challenges and strategies relevant to operational technologies. VELP has also been integrated with the xDome cybersecurity platform which is a tool that facilitates training in the fields of cybersecurity monitoring, threat detection, and vulnerability assessment capabilities, including CVSS scoring. It also supports cybersecurity compliance practices. As such, VELP not only uses this platform to keep itself cybersecure but also uses it for hands-on training purposes.

Last, VELP also equips its trainees from utilities and industries with practical, hands-on experience in applying cybersecurity compliance frameworks (e.g., NERC CIP, NIST CSF 2.0 [12], etc.), standards (e.g., IEC 62443, NIST SP800-82, etc.), policies, and other frameworks and guidelines (e.g., MITRE ATT@CK, D3FEND, etc.). Through immersive simulations and interactive modules, VELP allows participants to understand and implement crucial cybersecurity measures according to established guidelines and best practices. This practical approach helps trainees develop the skills needed to effectively navigate and apply cybersecurity protocols in real-world scenarios, enhancing their preparedness for cybersecurity compliance and operational challenges.

Conclusion and Future Work

In summary, VELP is available to support Canadians from diverse communities, including university students, newcomers, utilities, industries, and remote communities, with remote hands-on training programs in critical energy infrastructure and its cybersecurity using advanced tools and technologies such as digital twins and cloud applications. The Critical Infrastructure Cybersecurity Laboratory (CICL) and its associated Virtualized Experiential Learning Platform (VELP) are currently undergoing enhancements with the integration of the OT Companion, a new cloud-based cybersecurity and asset management solution. This upgrade is supported by additional funding from the Future Skills Centre, aimed at tailoring the training modules to meet the specific needs of diverse audiences, including remote communities, utilities, and industries.

The enhancements to the Virtualized Experiential Learning Platform (VELP) not only support critical skill development, but they also bolster the resilience of Canada's power and energy grids. By supporting research and development studies both currently and in the future, VELP is playing a crucial role in advancing the security and robustness of these essential systems. This initiative underscores the commitment to leveraging technology and education to improve infrastructure security across the nation

Looking ahead, there are plans to expand collaboration with other organizations and platforms that share similar goals to broaden hands-on training capabilities across Canada. Future developments for VELP also include the addition of more digital twins for specialized training areas such as EV charging infrastructure cybersecurity, Advanced Metering Infrastructure (AMI) and smart metering, IIoT, Virtual Power Plant (VPP), and advanced studies on Resilient Energy Systems. This expansion will enhance VELP's ability to provide comprehensive and practical cybersecurity training in critical energy sectors. Further, VELP will be expanded to support larger inter-provincial energy system interfaces and operation.

Acknowledgment

"Empowering Diverse Communities with Skills Development through Virtual Experiential Learning" is funded by the Government of Canada under the Future Skills program»

References:

[1] Eco Canada Labour Outlook, [Online]: https://eco.ca/new-reports/updated-environmental-labour-outlook-to-2025/

[2] Eco Canada, Demand for Clean Energy Job Growing, but is Canada Ready? October 2022, [Online]: https://eco.ca/blog/demand-for-clean-energy-jobs-growing-but-is-canada-

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

[4] Smart Microgrid Applied Research Team, [Online]: https://www.bcit.ca/applied-research/smart-microgrid/

[5] BCIT's Critical Infrastructure Cybersecurity Lab (CICL), [Online]: https://www.bcit.ca/smart-cicl

[6] Virtualization of Experiential Learning Platforms and their Pedagogical Models, FSC, July 2023, [Online]: https://fsc-ccf.ca/projects/virtualization-of-experiential-learning-platforms-and-their-pedagogical-models/

[7] Critical Infrastructure Cybersecurity Lab, British Columbia Institute of Technology, Hands-on engineering and configuration training in critical energy infrastructure areas, 2023, [Online]: https://references.siemens.com/en/reference/british-columbia-institute-of-techn?id=37043 Critical Infrastructure Cybersecurity Lab, British Columbia Institute of Technology, Hands-on engineering and configuration training in critical energy infrastructure areas, 2023, [Online]: https://references.siemens.com/en/reference/british-columbia-institute-of-techn?id=37043

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

[9] M. Manbachi, V. Vankayala, I. Letvenchuck, I. Ahmed, K. Mohammed, Virtualization Technology Applications in Advanced Digital Substations, CIGRE Canada Conference, CIGRE-600, September 2023.

[10] Minoo Shariat-Zadeh, Moein Manbachi, AD Barragán Gómez, Hassan Farhangi, Virtualization of the Experiential Learning Platform for Operation and Maintenance of Smart Microgrid Applications in Remote and Rural Communities in Canada, CIGRE Canada Conference, CIGRE-484, November 2022.

[11] M. Manbachi, J. Nayak, M. Hammami, A. G. Bucio, Virtualized Experiential Learning Platform for Substation Automation and Industrial Control Cybersecurity, in proc. 2022 IEEE Electrical Power and Energy Conference (EPEC), Victoria, BC, Canada, 5-7 December 2022.

[12] K. Stich, M. Manbachi, J. Nayak, V. Vanakayala, Analysis of a Digital Twin Model Power System Cyber-Attack to Develop a NIST Cybersecurity Framework Control Profile, CIGRE Canada Conference, CIGRE 583, September 2023.

About the Authors

Dr. Moein Manbachi is a Project Leader and Faculty with the Smart Microgrid Applied Research Team (SMART) within the Centre for Applied Research and Innovation of BC Institute of Technology in Vancouver. He was formerly a Post-doctoral Fellow at the Department of Electrical and Computer Engineering, University of British Columbia (UBC). Dr. Manbachi holds a Ph.D. degree in Mechatronic Systems Engineering from Simon Fraser University (SFU) and has 16+ years of experience in academia, industry, and R&D in the areas of Power Systems and Critical Energy Infrastructure Cybersecurity. He is the author/co-author of more than 60 technical papers published in high-ranked journals and conference proceedings. He is currently leading BCIT's critical infrastructure cybersecurity lab and serves as the project leader for the VELP initiative. Dr. Manbachi is an IEEE senior member and an active member of CIGRE and Engineers and Geoscientists of British Columbia (EGBC). His main research areas include but are not limited to Smart Grids, Advanced Substation Automation Systems, Critical Energy Infrastructure Cybersecurity, Power System Optimization, and applications of Digital Twin technologies in power systems.

Minoo Shariat-Zadeh **Minoo Shariat-Zadeh** is a Project Lead at the Smart Microgrid Applied Research Team (SMART) within the Centre for Applied Research and Innovation. With over 20 years of experience as an electrical engineer across the manufacturing, consulting engineering, and research and development sectors, Minoo serves as a team leader and a key contributor at SMART, where she is responsible for planning, organizing, designing, and executing applied research projects.

Her primary research interests include smart grids, smart microgrids, energy efficiency and conservation, alternative fuels for power generation and transportation, and renewable energies. Minoo holds a degree in Electrical Engineering from Azad University, Iran (IAU), and a Master of Engineering Leadership (MEL) in Clean Energy Engineering from the University of British Columbia (UBC), Vancouver. She also holds a Sustainable Energy Management Advanced Certificate (SEMAC) and is a certified RETScreen Expert.

Minoo Shariat-Zadeh is a member of Engineers and Geoscientists BC (EGBC) and a senior member of the Institute of Electrical and Electronics Engineers (IEEE).

Jay Nayak is a software engineer at BCIT, where he has developed web applications for Energy Management Systems (EMS) in smart microgrids and implemented user interfaces to educate communities in North America about the benefits of smart microgrids. He has also created cybersecurity models that focus on detection and mitigation strategies for cyber threats targeting Industrial Control System (ICS) protocols in critical infrastructure. Jay's professional experience includes designing and implementing scalable web applications for three Fortune Global 500 companies, a public organization, and two multinational corporations, working closely with cross-functional teams to ensure secure and efficient application deliveries. Jay holds a Master of Applied Science (MASc) in Electronic Systems Engineering from the University of Regina, where he also served as a Research Assistant. His research focused on cybersecurity in critical infrastructure, specifically on cyber vulnerability assessment and defense strategies for distributed generation in smart grid environments, resulting in a thesis, a journal paper, and two conference papers. His expertise encompasses cybersecurity research, threat modeling, security measures development, and software engineering skills, including full-stack web development, API design, and secure application deployment.

Mohamed Hammami is a Research Associate with the Smart Microgrid Applied Research Team (SMART) at the British Columbia Institute of Technology (BCIT). He specializes in cybersecurity for operational technology (OT) and has been working with the SMART team on OT implementation of VELP models for substations and Intelligent Electronic Devices (IEDs), adhering to ISA/IEC 62443 standards. Mohamed has extensive experience with industrial cybersecurity solutions, including segmentation of OT infrastructure, and creating educational labs for cybersecurity training. His technical expertise spans across various software, hardware, and cybersecurity tools, and he has been involved in research and development activities, contributing to publications on digital twin technology and cloud-based applications for critical infrastructure. He holds an Industrial Network Cybersecurity Diploma and is currently pursuing a Bachelor of Technology in Forensic Digital Cybersecurity at BCIT.

Dr. Vidya Vankayala is a Director of the Smart Microgrid Applied Research Team (SMART) at BCIT's Center for Applied Research and Innovation. In this capacity, he spearheads advanced research programs aimed at enhancing grid modernization and the resilience of energy systems, particularly focusing on developing a new smart grid innovation roadmap for BCIT and the province of British Columbia. With over 30 years of experience in both the utility and high-tech sectors, Dr. Vankayala has significantly contributed to grid modernization, distribution automation, microgrid development, and the cybersecurity of physical systems. His expertise extends to management consulting for electric utility transmission and distribution, and he has played pivotal roles in innovation as a Chief Architect, Solution Director, and Industry Specialist across various utilities. Dr. Vankayala is an active IEEE member, contributing to smart grid and smart city standards, and holds numerous publications related to smart infrastructure. Previously, he managed the High Power Lab at Powertech Labs Inc., enhancing services such as NERC CIP assessments and microgrid design. Dr. Vankayala's academic background includes a PhD in Electrical and Computer Engineering from the University of Calgary, and he has received substantial training in management

Teaching hands-on cyber incident response for SCADA network

Antoine Lemay
CYDEF
Montréal, Canada
antoine@cydef.ca

Michael Noory
CYDEF
Montréal, Canada
michael@cydef.ca

Felix Kwamena
Infrastructure Resilience
Research Group (IRRG)
Carleton Univeristy
Ottawa, Canada
Felix.Kwamena@carleton.ca

Andrew Lackey
Infrastructure Resilience
Research Group (IRRG)
Carleton Univeristy
Ottawa, Canada
AndrewLackey@cmail.carleton.ca

***Abstract*—With the increase of cyber incidents affecting critical infrastructure (CI) operations, such as the Colonial Pipeline ransomware incident, the need to develop cyber security skills in the CI workforce is high. However, because industrial control systems (ICS) are Cyber-Physical System (CPS) operating business critical infrastructure, opportunity to develop hands-on experience is limited, especially with regards to cyber attacks.**

With the use of a virtualized cluster replicating a SCADA network, we were able to provide an environment where cyber attacks could be safely run and operational impacts (the physical component of the CPS) could be observed.

This paper describes how virtualized sandboxes are used to emulate the cyber components and simulate the physical components to ensure suitable fidelity to show attack artefacts. The paper also highlights the need to optimize virtual machines to enable scaling to a classroom level. Finally, the paper discusses how to leverage the shared hosting to facilitate interactions with the trainees in a fully remote setting.

Keywords—Cyber-physical systems, Industrial control systems, cyber security

INTRODUCTION

As industrial control systems (ICS) become more and more automated, there is an increased convergence between operational technology (OT) and information technology (IT). This leads to increases in performance and reliability during the course of normal operations as real-time data and remote control can be used to optimize operations, respond to faults and perform maintenance.

However, with this increased convergence, cyber security risks were introduced into ICS. Examples such as the ransomware attack on the Colonial Pipeline [1] and some of the state-sponsored attacks against the Ukrainian power grid [2] illustrate how these risks can manifest. This means that cyber security expertise must be developed in industry practitioners to be in line with these new risks, particularly for operators of critical infrastructure (CI).

One of the main cyber security skills that must be train is the ability to perform early detection of cyber attacks and respond to cyber incidents. Having this skill helps to contain the damage and prevents the degeneration of incidents into crises. Unfortunately, because real cyber incidents are rare, it is difficult to get hands-on experience with this skill. After all, you would not want a power grid operator to infect their production systems on purpose to practice incident response.

Because ICS networks are cyber-physical systems (CPS), with the control components on the cyber side and the industrial process on the physical side, they are hard to reproduce in test or lab environments. As such, ICS operators cannot just train on non-production environments. Specialized training facilities including cyber ranges such as the one at Idaho National Laboratory [3] and the SANS Cyber City [4] are typically used to provide this kind of training. This type of cyber range is very effective for training in CPS because trainees can observe the physical consequences

of the cyber attacks. On the other hand, this approach requires physical access to the cyber range and provides limited scalability as the physical cyber ranges are expensive to develop.

In a country like Canada, where critical infrastructure is very geographically distributed, it is inconvenient to require trainees to travel to a dedicated facility, especially if the employee is performing an operation critical role. This problem was exacerbated by the COVID-19 pandemic. As such, as part of an initiative to increase resilience of Canada's energy infrastructure by providing training, the government of Canada decided to provide a session of remote hands-on training on cyber incident response for supervisory control and data acquisition (SCADA) networks, a specific type of ICS commonly used in the energy sector.

This paper presents an industrial experience report on the development and delivery of this training. The paper starts by providing the course outline and learning objectives to clarify the development requirements. Then, the training infrastructure's design is discussed. A brief overview of the remote experience and its challenged is included afterwards. Finally, results of the attendee survey and a conclusion are presented.

COURSE OUTLINE AND LEARNING OBJECTIVES

The course's target audience was employees of owner/operators of energy infrastructure as well as contractors who serviced the sector. The attendees were expected to have a working knowledge of IT and/or OT. The attendees were assumed to have limited cyber security knowledge as this was labelled an introductory course.

The overarching goal of the course was to provide lived hands-on experience with a cyber attack that could have operational impacts. The focus is on the processes needed to detect and respond to the attack. This was done because the process can be applied generally, while specific tools usually vary per company. Furthermore, commercial grade tooling usually relies on automating common tasks, which may make it more difficult for trainees to understand what is going on. For example, if a tool automatically generates alerts for anomalous processes via a closed source algorithm, learning the tool would not help a student understand what kind of processes should and should not be present.

The course was organised along one threat briefing presentation and four hands-on sessions over the course of three days. The threat briefing presented cases of real cyber attacks in the electricity sector to both establish the problem and highlight some commonalities. The 2015 attack on the Ukraine power grid is described in more detail as it will serve as the basis for the attack used in the hands-on session.

The first hands-on session had the attendees configure their own SCADA system. There were three goals to this session. First, it helped establish baseline knowledge of operational technology and terminology amongst the attendees. Most attendees where IT professionals that had increasing OT responsibilities, or OT professions with minimal understanding of the IT components, due to IT-OT convergence. Second, it provided the attendees with a way to familiarize themselves with the tools and infrastructure that would be used in the subsequent sessions. Third, it enabled the attendees to observe the systems operating in a clean state. This knowledge is critical to the detection tasks.

The second hands-on session had the attendees perform a basic cyber attack chain on the SCADA system they had built. This was to familiarize them with the process an attacker follows to achieve a compromise with an operational impact and to provide general awareness of what modern cyber attacks look like. The goal is also to cue in the attendees on the type of data artefacts that are left by this kind of cyber attack. This knowledge is also critical to the detection tasks.

The third hands-on session had the attendees follow a detection engineering process to build network detection rules that flagged attack artefacts without flagging normal operational activity. This is done by finding attack activity that sit outside of the constraints of normal operations. In the first session, the attendees had observed that the network traffic of OT networks were heavily constrained by the configuration, leaving

little room for attackers to move in an undetectable manner.

The fourth hands-on session had the attendees perform a host-based investigation following an intelligence lifecycle-based approach. Attendees are cued in to an attack from an initial detection. They must then use that detection to extract artefacts and mine them for information that will enable them to pivot to additional data sources and/or to filter down telemetry to a manageable subset in order to find relevant data from the attack. At the same time, the attendees get familiarized with the type of host-based artefacts that are left by cyber attacks.

In order to achieve these course objectives, the following are required:

- Ability to demonstrate the physical impact of a cyber attack
- Ability to execute realistic cyber attack chains
- High fidelity of normal OT system behaviour on the network level
- High fidelity of network attack artefacts
- High fidelity of host-based telemetry data volumes
- High fidelity of host-based attack artefacts

For example, if the network traffic was unrealistic or the network attack artefacts were not properly replicated, the attendees may not be able to replicate the detection engineering process in their own commercial environment. Similarly, if not enough non-relevant data is generated on the host, an attendee may bypass filtering and not learn this crucial skill.

This set of requirements informed our choices for the training infrastructure.

TRAINING INFRASTRUCTURE

As the instruction leans so heavily on the hands-on component, it was important to have a robust training infrastructure that fulfilled the requirements.

From the requirements, we can observe that the cyber component of the CPS requires very high fidelity, to ensure attack artefacts and normal baselining. On the other hand, the physical component of the CPS does not have the same fidelity requirements. The attendees need to be able to observe that their attack had an impact, but the exact physical values are not relevant.

As such, it is possible to use an approach similar to the one described in the paper on isolated clusters for SCADA network security research [5]. In particular, using the combined emulation and simulation approach enables us to achieve a high level of fidelity for the cyber components while keeping a reasonable fidelity on the physical component.

To emulate the environment, we used a hosted VMware ESX server. This enabled us to create virtual machines for all the cyber components we wanted to emulate. Furthermore, by using a hosted ESX, it was possible for us to be able to define virtual local area networks (vLANs) representing different network zones. The multi-zone setup was required to incorporate the crucial step of pivoting (and tunneling) in the cyber attack. This ability is unfortunately not available on many public hosted clouds such as Azure or AWS.

In this ESX server, we created a number of virtual machines and VLANs that recreate a corporate IT network, an OT network and a public network. These VMs are grouped in a “sandbox” that represent an individual unit that can be replicated. The exact composition of each sandbox will be described later.

ESX also offers remote access to the sandboxes in a secure manner. ESX allows user to connect to the server via password-protected web form (secured via HTTPS). It is possible to define role-based access control for individual virtual machines. Therefore, it was possible to create roles for the attendees that limited their access to the machines they would interact with and thus protect the attendees from altering the machines used in each sandbox’s infrastructure. The users can obtain full interactive access to the virtual machines via a web console or a VM remote control (VMrc) console. Because the VMs are hosted and the state is kept server-side, this method of access has the benefit of allowing

multiple people at different locations to see and interact with the same machine.

When building the sandbox, there is again a trade-off between fidelity and scalability. Normally, corporate networks are very large and use a host of technologies. Similarly, OT networks include a fair diversity of items. However, the more machines are emulated, the bigger the storage and memory footprint of a sandbox. This means that it becomes more difficult to replicate the sandbox to accommodate more students.

Going back to the model attack we wanted the attendees to replicate (Ukraine 2015), the attack chain started with a spear phishing email, followed by a device compromise, lateral movement to compromise the domain and finally tunneling to the OT system. Once a pivot point was established to the OT system, malware was deployed on controllers (PLCs) and "ghost mouse" (full GUI remote control) of human machine interface (HMI) machines was used to create physical impact. Because the domain component required the addition of a domain controller (and multiple machines for the privilege escalation), we decided to exclude this component. Also, since the PLC exploitation component was too advanced for an introductory course, this part was dropped as well.

In order to be able to replicate the critical parts of the attack chain (except the ones that were cropped), we built the following virtual machines:

- Attacker machine (Kali Linux)
- Firewall/router machine (pfSense)
- Infrastructure machine (mail, DNS)
- Physical simulation machine (RTUs, simulator)
- Master Terminal Unit (MTU)
- Operator workstation (HMI, mail client)
- Security Onion (network monitoring)

The attacker machine and the infrastructure machine were located in the public network VLAN, the MTU, the Security Onion and physical simulation machine were located in the OT VLAN. The operator workstation was dual homed (to illustrate a common vulnerability) and had one network port in the IT VLAN and one network port in the OT VLAN. The firewall had one port in each VLAN to allow routing between the networks. Figure 1 illustrates the network used for each sandbox.

To minimize costs, open-source software was used whenever possible. For the attacker machine, Kali Linux and the Metasploit framework were used to replicate the spear phishing malware implant payload. For firewalling and routing, a pfSense distribution was used. For infrastructure, Bind was used for DNS and postfix for mail on an Ubuntu server. For network security monitoring, Security Onion and Snort were used. The physical simulation machine used python scripts leveraging the modbus-tk library [6] to emulate the RTU and another python script to act as the physical system simulation program. These scripts were running on a minimal Archlinux distribution to save on the memory footprint. Furthermore, multiple network interfaces were assigned to the machine to emulate the presence of multiple remote terminal units (RTUs) and create the semblance of scale without augmenting the memory footprint. The master terminal unit machine and the operator workstation machine were both Windows machines for verisimilitude of attack artefacts. However, additional software running on these machines was open source. Notably, a version of SCADA BR [7] open MTU program was used to replicate the master terminal unit software and database, as well as the historian software. The human machine interface (HMI) software was a web application provided by SCADA BR and accessed via a web-browser from the operator workstation. The SCADA protocol used was Modbus over TCP/IP as it has been open-sourced. The network protocol was the most impactful concession to costs as it is not a protocol used commonly in production systems anymore and it is used in a high fidelity context for detection engineering. However, many of its core characteristics (master/slave architecture, polling-bases state estimation, lack of authentication, etc.) are shared by numerous commercial protocols today.

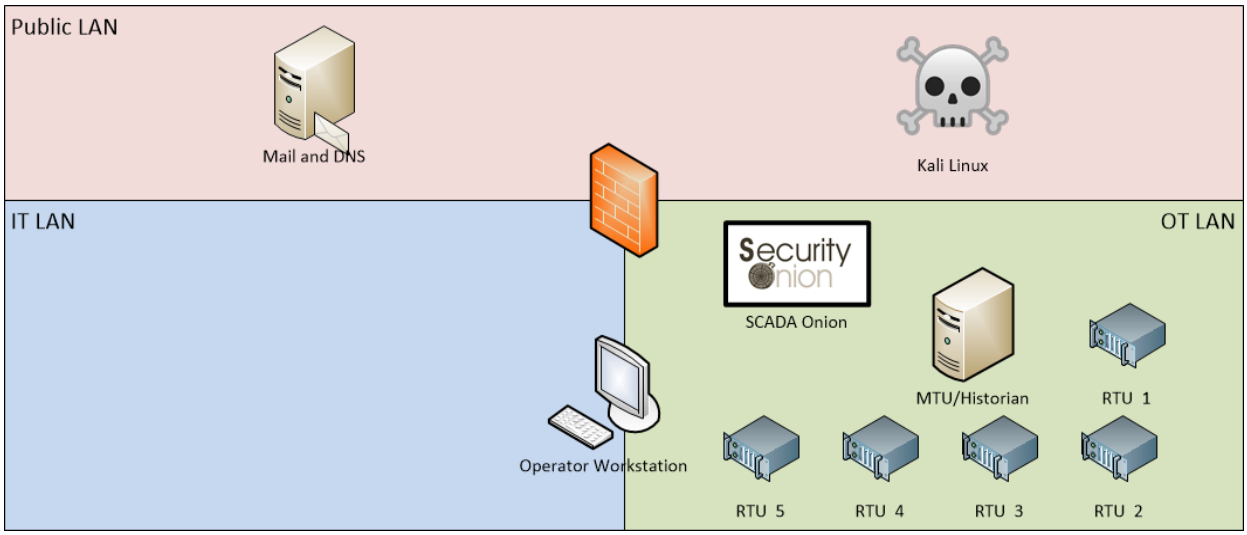

Fig. 1. Network map used in the exercise

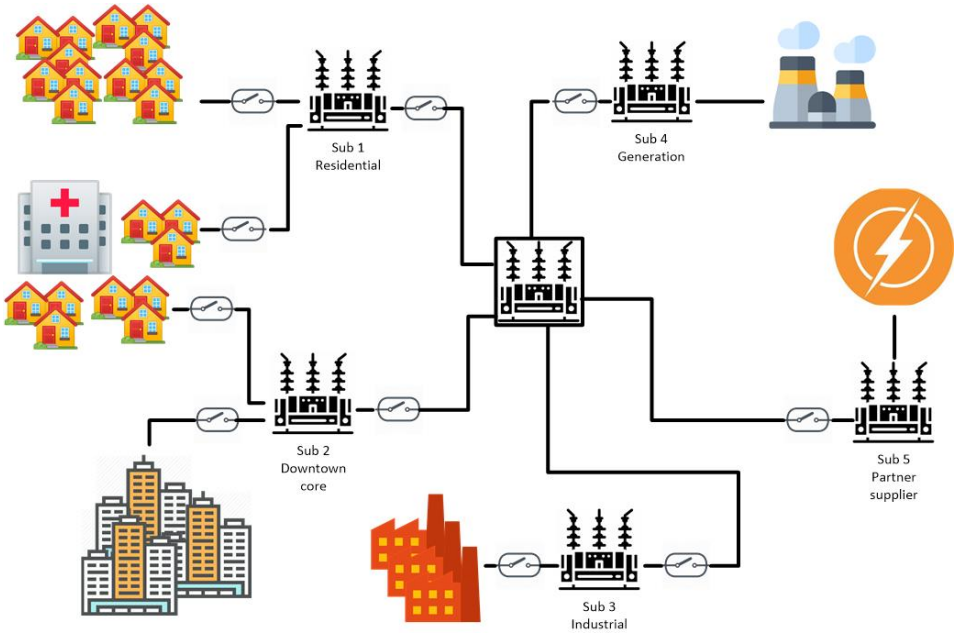

Fig. 2. Electrical map used in the exercise

In terms of the physical system simulation, because the fidelity requirements were quite low, we opted for a simple script that provided the preservation of energy between the electricity generation sources and the electricity consumption sinks. This had the benefit of being able to generate enough measurements to populate the small-scale SCADA network included in the exercise, while keeping session development costs low. It also provided easily understandable points of actions for attendees who did not possess a good understanding of power systems: by turning the breaker(s) coming from the power generation lines off, the power would go down in the power consumption areas. Therefore, they could easily replicate the impact achieved in the 2015 attack on the Ukrainian power grid. A map of the electrical system is provided in Figure 2.

From all these considerations, we managed to get each sandbox to 18.25 GB of RAM and about 120 GB of SSD storage. This means that we could run around 9 sandboxes on one rented server that cost us around

Can$ 1000 per month (including the overhead for running the VMs). When working with directed hands-on labs, our experience indicates that the optimal number of people per sandbox is two. One attendee can use the instructions to follow along and direct. The other attendee can perform the technical tasks. This keeps both attendees engaged and communicating. It also allows the attendees to bounce ideas off each other. This is particularly true in cases where there is a wide initial knowledge disparity within groups. As you add individuals to the group, these individuals have no ongoing tasks, which makes it harder for them to be engaged. As such, our setup could comfortably accommodate 18 attendees and could provide a reasonable experience for up to 27 attendees.

REMOTE EXPERIENCE

While the infrastructure allowed the attendees to perform the required tasks remotely, there were still a few challenges for remote instruction.

The first challenge is one of attendee communication and coordination. While the hosted virtual machine shared a state between all the attendees, they had to make sure they could follow what was going on while someone else was working, be able to ask questions of their teammates and instructors, and generally avoid stepping on each other's toes while working with the shared resources.

The solution we used for the purpose of this training was to use Discord [8]. Discord is a communication tool that allows for Discord allows for voice, video and text chat in a multi-channel setting. This means we could create channels for plenary discussions or group-wide data diffusion, but also have the ability to create smaller break-out rooms for individual groups. Discord is "server"-based, meaning that a server is created for a community and the data for that community is persistent. This means that it is possible for users to interact with Discord in an asynchronous manner, for example posting a comment outside of the normal training hours, so that it is read when convenient for the recipient. Furthermore, this allows for easier archival of conversations, which was a requirement by the government sponsor.

Finally, Discord also has the ability to stream the screen of one or multiple people in a channel. Individuals see all the different streams available and can select which one(s) they want to see. This removes a layer of coordination from typical office meeting applications where only one person can share screen at a single time.

The main issue with Discord is that the platform was initially developed with computer gaming in mind. As such, it is blocked in many corporate organizations. This created a challenge for multiple attendees who got the connection instructions a few days before the start date and either could not initially join or had to use a personal device instead of their work computers. Furthermore, while the screen streaming service allows for smooth high-quality file sharing (often required to be able to read on screen text), the bandwidth requirements was too great for at least one attendee.

While coordination and communication between attendees of the same group is fairly well managed, communication and coordination with the trainer is more challenging in a remote setting. For directed hands-on session, in a live setting, it is possible for the trainer to walk around and look at what attendees are doing to ensure they are in-line with what they are supposed to do. It is also possible for the trainer to listen to communications between the attendees to get a heads up when a group is struggling. This is generally not possible in a remote setting. While the trainer can be proactive to a certain degree by using either VMWare or Discord stream to check on team progress, it is not possible to anticipate problems through overhearing conversations (unless the problem is being discussed in the channel the trainer is in). As such, it is very important to prime the attendees to ask questions early and often. A number of cases where groups struggled for too long before asking a question and not being able to fully complete a session occurred.

Another major challenge of remote training is the management of trainee attention. One of the advantages on on-site training in relation to remote training is that

there are less work-related distractions. So, it is easier for the trainer to have somewhat of a monopoly on the attendees' attention (especially in facilities where cellphones are not allowed). However, during remote training, it is very easy for attendees to perform other tasks on the side or be sidetracked by other priorities at work. If the training was fully individualized, this would not be that much of an issue. After all, if the trainee wastes the time spent in training, they will have to answer to their respective companies. However, it becomes more problematic when teammates get stranded without partners if group work is expected.

Based on the experience of this training, no good solution was found for this issue. Proactive team reshuffling, where stranded attendees were paired with other stranded attendees and users with similar behaviour patterns were paired with each other alleviated the worst of the problem. However, some groups consistently struggled to complete hands-on sessions because of this issue. It should also be noted that this was probably considered a benefit from some of the attendee's viewpoint. It is difficult for critical personnel to take time completely away to attend training. So, having the ability for partial participation in a training activity is a massive improvement over no possibility of training.

SURVEY RESULTS

Even with all the challenges from remote training, the attendees appear to have enjoyed the training. A survey was sent to the participants so they could rate their experience and evaluate the impact of the government program.

As a start, the session was greatly oversubscribed. 29 participants attempted to register, but participation was capped at 19 participants, making the sessions 147% oversubscribed. This compares very favourably to the participation of in-person sessions that were offered before the pandemic. While it is not possible to know if this is because of new actors cycling in and out of industry (the previous in-person training having had multiple successive classes, depressing turnout in later ones), or because the ability to do the training remote proved more compelling. However, anecdotally, there appeared to be more attendance from British Columbia, the province that is the most remote from the physical training site.

Then, of the people that answered the survey, the overall rating accorded to the session was 4.8/5, 94% were likely to recommend the training to their colleagues and 100% said they felt better prepared to detect, respond and recover from cyber attacks. These numbers show a great level of appreciation from the attendees, even through the challenges of being remote.

Naturally, since the attendees self selected whether to answer the survey or not, we should expect a significant sampling bias in the results. As such, the fact that a large number of net promoters decided to answer the survey is not surprisingly. However, it should be noted that people with strong negative opinions also generally self-select to answer this kind of survey to make their concerns heard. The fact that there does not appear to be one is significant.

CONCLUSIONS

Based on the student's appreciation of the course, it appears that remote training is a viable option for professional training of cyber incident response skills in industrial control systems. This represents an opportunity to address a skill gap that is growing with the increased convergence between IT and OT because remote training is inherently more scalable than in-person training in a dedicated facility.

Some of the technical challenges of remote training on CPS systems can be overcome by adopting a hybrid emulation/simulation approach, where components requiring a high level of fidelity to achieve the learning objectives are emulated and the components that require a low level of fidelity are simulated. This implies that more thought needs to be put in the class design to define requirements and build to purpose.

Another level of optimization can also be achieved by replacing commercial tools with open-source software and/or by combining multiple components on a single virtual machine when the loss of fidelity will

not hurt the learning objectives. This has the added benefit of helping with the scalability of classes in relation to hardware costs.

In addition to these technical challenges, there are also communication and coordination challenges to remote training. While some of them can be alleviated using modern communication platforms and services, others are more difficult to tackle. Notably, the challenge of attendees getting pulled away by other work tasks is greatly exacerbated in remote sessions. This makes the work of the trainer more difficult, even if this can be considered a benefit by some attendees who cannot usually take time off work to attend full days of training.

In that sense, we believe this experience with remote training for cyber incident response has been positive and could be replicated in the future. Furthermore, it may serve as an inspiration for other hands-on training in areas where there is little opportunity to get lived-in experiences. For example, in cyber-physical training courses where it is difficult for trainees to get their hand on physical components.

REFERENCES

[1] W. Turton and K. Mehrotra, "Hackers Breached Colonial Pipeline Using Compromised Password," 4 June 2021. [Online]. Available: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password. [Accessed 20 March 2023].

[2] K. Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, 3 March 2016. [Online]. Available: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/. [Accessed 29 January 2019].

[3] "Workforce Development & Training," U.S. Department of Energy, [Online]. Available: https://inl.gov/national-security-training/. [Accessed 20 March 2023].

[4] R. J. O'Harrow, "CyberCity allows government hacker to train for attacks," 26 November 2012. [Online]. Available: http://www.washingtonpost.com/investigations/cybercity-allows-government-hackers-to-train-for-attacks/2012/11/26/588f4dae-1244-11e2-be82-c3411b7680a9_story.html. [Accessed 20 March 2013].

[5] A. Lemay, J. Fernandez and S. Knight, "An isolated virtual cluster for SCADA network security research," in *1st International Symposium for ICS & SCADA Cyber Security Research 2013 (ICS-CSR 2013)*, Leicester, 2013.

[6] L. Jean, "modbus_tk 0.4.3," Python Software Foundation, 3 November 2014. [Online]. Available: https://pypi.python.org/pypi/modbus_tk. [Accessed 6 May 2015].

[7] Sourceforge, "Sourceforge project - SCADA BR," 16 December 2014. [Online]. Available: http://sourceforge.net/projects/scadabr/. [Accessed 26 January 2015].

[8] Discord, "Discord | Your place to talk and hang out," [Online]. Available: https://discord.com/. [Accessed 20 March 2023].

[9] T. Proffitt and A. Abdel-Aziz, "Scoping Security Assessments - A Project Management Approach," 2011. [Online]. Available: https://www.sans.org/reading-room/whitepapers/auditing/scoping-security-assessments-project-management-approach-33673.

[10] Joint Task Force Transformation Initiative, "SP 800-53A Rev. 4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans," 10 December 2014. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-53a/rev-4/final.

[11] The Economist Intelligence Unit, "The Meaning of Security in the 21st Century," 2017. [Online]. Available: https://perspectives.eiu.com/sites/default/files/The-meaning-of-security-in-the-21st-century1.pdf.

[12] The American Petroleum Institute and National Petrochemical and Refiners Association, "Security Vulnerability Assessment Methodology," 2003. [Online]. Available: https://www.nrc.gov/docs/ML0502/ML050260624.pdf.

[13] The American Petroleum Institute and National Petrochemical and Refiners Association, "Security Risk Assessment Methodology," 2013. [Online]. Available: https://www.researchgate.net/publication/259137244.

[14] Office for Domestic Preparedness, "Vulnerability Assessment Methodologies Report," 2003. [Online]. Available: https://www.hsdl.org/?abstract&did=449166.

[15] M. Lupacchino, " Security Assessment vs. Security Audit," 2015. [Online]. Available: https://info.focustsi.com/IT-Services-Boston/topic/data-security/Security-Assessment-vs-Security-Audit.

[16] T. R. Brewer, J. E. Crawford, P. J. Vonk and L. M. Torres, "A quantitative approach to physical security assessments for power & energy infrastructure," in *North American Power Symposium*, Charlotte, NC, 2015.

[17] The German Federal Office for Information Security, "A Penetration Testing Model," [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.pdf?__blob=publicationFile&v=1.

[18] T. Dimkov, W. Pieters and P. Harte, "Two methodologies for physical penetration testing using social engineering," 2009. [Online]. Available:

https://research.utwente.nl/files/5097052/Pentesting_methodology.pdf.

[19] Souppaya, M. P. and K. A. Scarfone, "Technical Guide to Information Security Testing and Assessment - Recommendations of the National Institute of Standards and Technology," 2008. [Online]. Available: https://www.nist.gov/publications/technical-guide-information-security-testing-and-assessment.

[20] B. Hart, "Implementing a Successful Security Assessment Process," 2001. [Online]. Available: https://www.sans.org/reading-room/whitepapers/basics/implementing-successful-security-assessment-process-450.

Short Review of Machine and Deep learning Advancements in Wildfire Management

Aziz Al-Najjar, Marzieh Amini, James R Green, Felix Kwamena, Carleton University

Abstract—Recent wildfire seasons in Canada have reached un precedented levels, burning millions of hectares and threatening critical infrastructure. This paper reviews the advancements in machine learning (ML) and deep learning (DL) technologies for wildfire management, emphasizing their transformative role across pre-fire, active-fire, and post-fire stages. In pre-fire management, ML and computer vision techniques enhance fuel type classification, reducing fire hazards. For active-fire management, DL models improve real-time fire detection and mapping, enabling efficient resource allocation and community protection. Post-fire, ML and DL methods facilitate accurate burned area and fire severity mapping, supporting effective recovery efforts. By integrating these technologies, the paper highlights current capabilities and future directions in wildfire management, aiming to bolster infrastructure resilience and safeguard human lives.

I. INTRODUCTION

Canada's recent wildfire seasons have been extraordinarily severe, setting new records in terms of area burned and intensity. In 2023 alone, wildfires consumed over 17.3 million hectares, a significant increase from the 10-year average of 2.2 million hectares as shown in Fig. 1 [1]. This escalation is attributed to prolonged drought conditions across several regions including British Columbia, the Prairies, the Northwest Territories, and northern Ontario, fueling unprecedented fire activity [1]. The impact on infrastructure has been consider able, with numerous communities facing evacuation orders and extensive property damage. The fires have not only threatened the immediate safety of these areas but also posed long term challenges to rebuilding and reinforcing infrastructure resilience against future wildfires. This situation highlights the critical need for enhanced fire management strategies and infrastructure planning to mitigate the growing threat posed by such natural disasters in Canada and globally [2]

The escalating wildfire incidents in Canada not only imperil vast stretches of land but also pose severe threats to the robustness of critical infrastructure. As observed in recent wildfire seasons, the interplay between human activities and natural vegetation contributes significantly to fire behavior. Notably, the proximity of flammable vegetation and the expansion of human settlements into fire-prone areas complicate the dynamics of fire spread, necessitating advanced approaches to infrastructure protection and disaster response.

Enhancing infrastructure resilience against wildfires is paramount. It involves fortifying structures, ensuring that utility networks can withstand fire exposure, and implementing smart landscaping to reduce fuel availability near critical assets. This approach also demands adaptive management strategies that utilize real-time data to optimize responses and minimize potential damage to infrastructure, thereby ensuring continuity in essential services during and after wildfire events.

Transitioning into technological solutions, the role of ma chine learning (ML) and computer vision becomes crucial. These technologies offer transformative capabilities in detecting and analyzing wildfires, enabling preemptive actions that could mitigate the impact on infrastructure. ML algorithms can analyze vast datasets from satellite imagery and ground sensors to predict fire spread patterns and potential impacts on specific infrastructures. Meanwhile, computer vision techniques enhance surveillance and monitoring systems, providing detailed and accurate real-time visuals of fire-affected areas. Such advanced technologies facilitate efficient resource allocation, targeted firefighting efforts, and strategic evacuation plans, thereby bolstering community resilience against the devastating effects of wildfires.

The subsequent sections of this paper will begin by dis- cussing previous work by the authors in identifying vegetation encroachment areas on powerlines, which is a critical aspect of wildfire prevention. Building on this foundation, the paper will then focus on Fuel Type Classification as a key component of pre-fire management, emphasizing the role of ML and com puter vision techniques in proactively managing vegetation and reducing fire hazards. The discussion will progress to the Fire Detection and Mapping in Active Fire Management, where the paper will explore

advanced models and technologies used to detect, monitor, and respond to wildfires in real time. Finally, the paper will address Burned Area and Fire Severity Mapping in Post-Fire Management, highlighting the use of ML and DL methods in assessing fire impacts and guiding recovery efforts. Through a comprehensive exploration of these technologies, the paper aims to present a cohesive overview of current capabilities and future directions in wildfire management, with a focus on enhancing the resilience of critical infrastructure and safeguarding human lives.

II. IDENTIFYING VEGETATION ENCROACHMENT AREAS ON POWERLINES

The paper titled "Identifying Areas of High-Risk Vegetation Encroachment on Electrical Powerlines Using Mobile and Air borne Laser Scanned Point Clouds" [3] focuses on developing a robust methodology to detect vegetation encroachment on powerlines, a critical factor in preventing power outages and wildfires, particularly in complex urban environments. This study addresses the unique challenges posed by high-density urban settings, which complicate the accurate classification of powerline and vegetation points due to the presence of various urban structures.

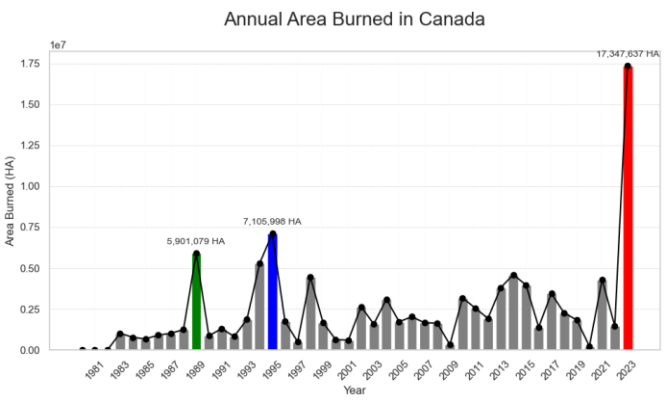

Fig. 1. Annual Area Burned in Canada [1]

The proposed methodology consists of a two-stage approach to accurately and automatically detect vegetation encroachment. In the first stage, the method classifies the points in the point cloud into three categories: vegetation, powerline, or background. This classification leverages deep-learning models, with the study comparing PointCNN and RandLANet, ultimately selecting RandLA-Net due to its superior performance in both mobile laser-scanned (MLS) and airborne laser-scanned (ALS) datasets. The second stage involves the novel point-based encroachment detection (P-BED) algorithm, which precisely identifies encroachment areas by analyzing the proximity between vegetation and powerline voxels in the point cloud. The P-BED algorithm utilizes techniques such as map sectioning, voxel-based down sampling, and proximity analysis to achieve highly accurate results.

The effectiveness of this two-stage methodology is demonstrated through impressive performance metrics, achieving F1- scores of 0.98, 0.96, and 0.94 for classifying background, vegetation, and powerline points, respectively, and achieving 100% precision and 96.0% recall for encroachment detection. Figure 2 illustrates the results for Walkley Road, Ottawa, Ontario where the purple areas indicate severe vegetation encroachment, and the pink areas show minor encroachment. This visual representation underscores the practical utility of the proposed method in urban vegetation management and proactive maintenance.

By integrating advanced Deep Learning (DL) models and innovative detection algorithms, this work offers a significant contribution to urban wildfire prevention strategies, providing a scalable and precise tool for managing vegetation encroachment on powerlines. Future research directions may focus on enhancing the model's generalizability across diverse datasets and optimizing real-time application capabilities

III. PRE-FIRE MANAGEMENT: FUEL TYPE MAPPING

Effective wildfire management begins long before the first flames ignite. The behavior of wildfires is influenced by a complex interplay of factors such as weather conditions, topography, and particularly vegetative fuel, which presents a significant opportunity for forest management and ecological restoration aimed at reducing fire hazards [22]. To mitigate these risks proactively, several measures can be employed. These include thinning trees to break up continuous canopies and fuel ladders, conducting prescribed burns to reduce fuel loads and restore the ecological role of fire, and removing invasive, non-native species that exacerbate fire risks [23]. Implementing these solutions well in advance of fire events is crucial and requires the adoption of proactive, data-driven strategies. This section introduces several AI-enabled solutions for fuel monitoring, which

enhance the effectiveness and accuracy of pre-fire management measures. These technological advancements facilitate the early implementation of strategies, shifting from traditional labor-intensive practices to more efficient, AI-driven approaches.

A. Fuel Type Mapping and Classification Systems

Accurate fuel type mapping is essential for assessing wildfire risks and predicting fire behavior. By understanding the specific vegetation characteristics within an area, managers can effectively plan and implement targeted strategies to reduce the likelihood and impact of wildfires [24]. Various fuel type classification systems have been developed worldwide, including the Canadian Fire Behavior Prediction (FBP) System [4] and the Northern Forest Fire Laboratory (NFFL) system [5]. These models provide a framework for categorizing vegetation types based on their fire behavior characteristics, aiding in wildfire risk assessment and management.

B. Limitations of Traditional Classification Systems

While traditional fuel type classification systems have been instrumental in wildfire management, they come with notable limitations. These systems are often complex and expensive, with their structural variability leading to site-specific applications that may not be adaptable across different geographic regions [25]. Additionally, the dynamic nature of fuel types, which can change over time due to environmental disturbances, necessitates frequent updates to maintain accuracy in fire risk management. This poses significant challenges in cost-effective updating, underscoring the need for AI-driven solutions that offer greater adaptability and efficiency [26].

C. ML Techniques

Traditional pixel-based methods, such as neural networks (NN), support vector machines (SVM), and maximum likelihood classifiers, have been extensively used for fuel type classification [7], [8], [27]. These techniques treat each pixel independently, without considering spatial interactions, often leading to a “salt and pepper” effect in the classification results [8]. While widely adopted, these methods can produce noisy outputs due to the lack of spatial context, resulting in less accurate and sometimes misleading classifications.

D. Object-Based Image Analysis

Object-Based Image Analysis (OBIA) offers an alternative to pixel-based methods by integrating textural, spatial, and spectral information into the classification process through multi-scale image segmentation. OBIA has been particularly

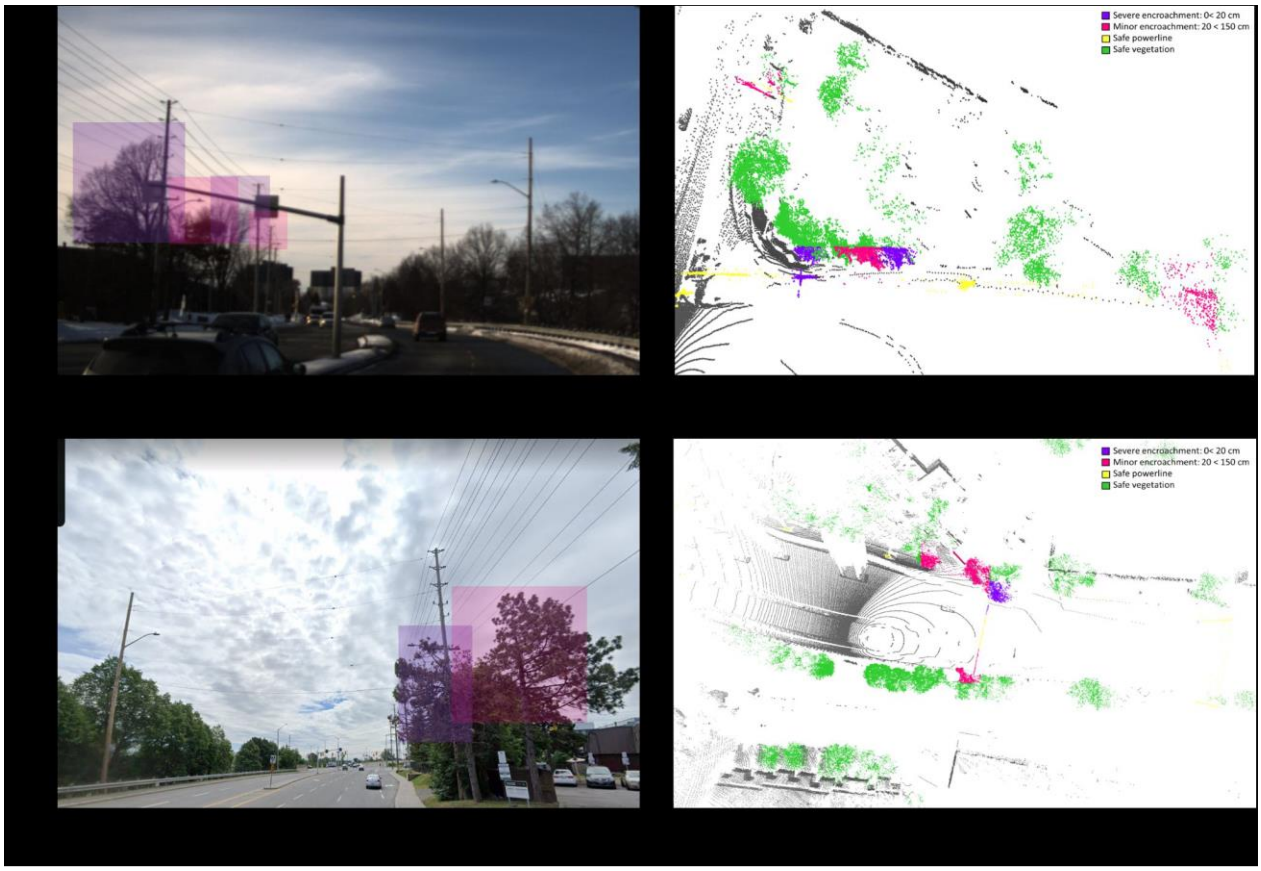

Fig. 2. Encroachment areas of Walkley Road: Purple areas represent the areas where vegetation has severe encroachment, and pink areas show minor encroachment. Note: the highlighted areas in the camera frames were manually highlighted for illustrating purposes

effective in improving classification accuracy when applied to very high-resolution (VHR) images for fuel type mapping [28]. By incorporating multiple types of information, OBIA significantly enhances the accuracy of fuel type classification compared to traditional pixel-based approaches. However, the complexity of OBIA, including the need to select appropriate scales for image segmentation and the correct features for classification, makes it challenging and resource-intensive to implement [29].

E. DL Architectures

Recent advancements in DL, especially in deep convolutional neural networks (CNNs) and Vision Transformers (ViT), have revolutionized fuel type classification in remote sensing. CNN architectures excel in feature extraction, making them highly effective for mapping fuel types [15], [16]. These advanced DL techniques address the inefficiencies and time-consuming nature of conventional ML algorithms by automatically generating meaningful representations of complex data [17], [30], [31]. Furthermore, DL approaches, such as spectral unmixing combined with classification tasks, have been developed to efficiently analyze the rich spectral and spatial information contained in hyperspectral images [32] and LiDAR data [28]. This integration enhances the performance of fuel type classification by amplifying the training set and simplifying the classification process. However, despite their superior performance and efficiency, DL models require large datasets to prevent underfitting, which may not always be available. Additionally, these models are computationally intensive and data-hungry, posing challenges in terms of resource requirements and scalability.

IV. ACTIVE-FIRE MANAGEMENT - FIRE DETECTION AND MAPPING

Once a wildfire ignites, it is crucial to implement advanced methodologies for monitoring and management, as the fire's size and complexity can escalate rapidly. Timely responses are essential to contain fires while they are still small and manageable. Traditionally, fire detection has relied heavily on human observers using visual cues, either directly from fire towers or through video feeds from towers, aircraft, or ground-based cameras [6]. However, these methods are constrained by several limitations, including restricted spatial and temporal coverage, the potential for human error, interference from smoke from other fires, and dependency on daylight conditions.

To address these challenges, ML and DL-based computer vision methods have emerged as powerful tools. These technologies significantly extend coverage, enhance detection efficiency in smoky conditions, and eliminate the biases associated with human observation [33], [34]. Automated systems in this context typically involve the analysis of infrared (IR) or optical images to detect heat signatures or smoke, framing the detection problem as a classification task ideally suited to ML approaches [35].

This section will explore common computer vision-based methods for fire and smoke detection, as well as techniques for wildfire monitoring, tracking, and control. These advanced models play a pivotal role in active-fire management, enabling more effective and timely interventions.

TABLE I
COMPARISON OF TRADITIONAL METHODS, ML, AND DL IN WILDFIRE MANAGEMENT

Method	Pre-Fire Management: Fuel Type Classification	Active-Fire Management: Fire Detection and Mapping	Post-Fire Management: Burned Area and Fire Severity Mapping
Traditional Methods	• Advantages: Established models like the Canadian FBP and NFFL systems are well-validated and widely adopted [4], [5]. • Disadvantages: Often lacks spatial context, leading to potential inaccuracies in fire behavior predictions.	• Advantages: Human observers can provide immediate, real-time detection with minimal technology requirements. • Disadvantages: Limited by daylight, prone to human error, and restricted spatial/temporal coverage [6].	• Advantages: Simple, direct methods for mapping burned areas, such as GPS and aerial surveys. • Disadvantages: Labor-intensive, time-consuming, and often lacks precision.
ML-based methods	• Advantages: More accurate classification by integrating various data sources; handles complex datasets [7], [8]. • Disadvantages: Can produce noisy outputs due to lack of spatial context; requires substantial data preprocessing [8].	• Advantages: Capable of processing large datasets with higher accuracy and faster detection than traditional methods [6], [9]. • Disadvantages: Requires large, high-quality labeled datasets; performance can degrade with poor data quality [10].	• Advantages: Effective for predicting burned area and assessing fire severity; handles complex relationships well [11], [12]. • Disadvantages: Computationally intensive and can struggle with parameter tuning; may not generalize well across different regions [13], [14].
DL-based methods	• Advantages: Excels in feature extraction and can automatically learn from raw data, leading to highly accurate classifications [15], [16]. • Disadvantages: Data-intensive and computationally demanding; requires large datasets to avoid underfitting [17].	• Advantages: Superior in detecting and mapping fire and smoke; can handle spatial and temporal data with high accuracy [18], [19]. • Disadvantages: Resourceheavy and may require specialized hardware; less effective with small datasets [9].	• Advantages: Provides detailed and accurate burned area and severity maps; suitable for large-scale, automated tasks [20], [21]. • Disadvantages: High computational costs; struggles with generalization across different landscapes without diverse training data [20].

A. ML-Based techniques

ML based fire detection models employ a variety of algorithms to analyze data from sensors, images, and other sources to detect the presence of wildfires. These models include techniques such as Artificial Neural Networks (ANNs) [6], [10], [35], [36], Support Vector Machines (SVMs) [9], Tree based methods [37]–[39], Bayesian Networks (BN) [40], Adaptive Neuro-Fuzzy Inference Systems (ANFIS) [41], and K-Nearest Neighbors (KNN) [38]. ANNs are commonly used for processing infrared (IR) imagery combined with visual data and meteorological inputs, as demonstrated by [6], who have developed systems capable of detecting wildfires by analyzing multiple attributes like flame, heat, light, and radiation. SVMs are also popular for analyzing video frames to automatically detect wildfires [9], while Genetic algorithms have been applied for optimizing LiDAR-based fire detection systems [42].

The main advantage of ML-based fire detection models is their ability to process and analyze large datasets from multiple sources, providing more accurate and timely detection compared to traditional methods. They can handle complex relationships between variables and offer flexibility in integrating different types of data, making them suitable for diverse wildfire scenarios. However, these models also have some limitations. They often require significant amounts of high quality labeled data for training, which may not always be available [10]. Additionally, the effectiveness of these models can be influenced by the quality of the input data, and they may struggle with generalizing to new, unseen conditions. Despite these challenges, ML-based methods remain a powerful tool in the early detection and management of wildfires, providing a solid foundation for more advanced DL approaches.

B. DL-Based Techniques

DL models, CNNs, have become essential in fire detection and mapping, exhibiting superior capability in feature extraction from spatial images. These models are utilized extensively in tasks such as fire and smoke detection, mapping, and predictive analysis. Unlike traditional ML methods, CNNs excel at learning complex patterns from raw data, adeptly handling the spatial variability typical in fire scenarios.

Specific applications include training on terrestrial-based images to detect fire and smoke. For instance, [18] and [34] showed that incorporating time-dependent information significantly enhances detection accuracy. [43] used a three dimensional approach to segment smoke in video images. Another breakthrough involved integrating CNNs with Long Short-Term Memory (LSTM) networks to improve sequence 5 image analysis, as demonstrated by [19], who achieved a 97.8% accuracy rate.

For UAV and satellite imagery analysis, comparisons of SVM, ANN, and CNN models [9] revealed that 15-layer architecture outperformed others, achieving 98% accuracy. CNNs have also proven effective in large-scale fire management using satellite data, with the YOLO ”You Only Look Once” model noted for its speed and accuracy over region based methods, emphasizing the efficiency of certain DL architectures in time-sensitive applications [44].

Recent advancements include vision transformers like TransUNet and TransFire, which excel at extracting detailed features from aerial images and address challenges such as background complexity and small fire areas [45], [46]. These models have achieved F1-scores of 99.9% and 99.82%, respectively, surpassing many traditional architectures.

The main advantage of DL methods, including those using CNNs and transformers, lies in their robust feature-learning capabilities from extensive datasets, ensuring high accuracy even under complex conditions. They process data from diverse sources, capturing both spatial and temporal dimensions. However, the resource-intensive nature of these models, requiring substantial computational power and large labeled datasets, poses challenges. Additionally, their performance may struggle in new environments without diverse training data.

V. POST-FIRE MANAGEMENT - DAMAGE ASSESSMENT AND RECOVERY MONITORING

In the aftermath of wildfires, a critical step is the prompt and effective assessment of the damage to understand both the economic and ecological impacts. This assessment is essential for informed recovery planning and for mitigating future risks. Historically, methods such as ground surveys, aerial GPS, and air-photo interpretation were employed to map burned areas and evaluate burn severity [47]. However, with the advent of advanced technologies, these traditional techniques have been significantly improved. In this

section, we discuss the advancements by ML that have enhanced postfire management. These ML-driven approaches offer increased accuracy and efficiency in mapping burned areas and assessing burn severity, providing vital insights for the restoration and management of fire-affected landscapes.

A. Burned-Areas and Fire Sevirity Mapping

ML and DL methods have been extensively utilized for mapping burned areas and assessing fire severity following wildfires, offering significant advancements over traditional approaches. Early studies in ML-based burned area mapping employed techniques such as ANNs, logistic regression (LR), SVM, and KNN to map burn scars and assess fire severity using satellite imagery. For example, [13] utilized ANNs for burn-scar mapping and fire detection, while [14] compared LR with ANN for mapping using Landsat images, achieving high accuracy (97%). SVM has been particularly successful in this domain, outperforming other ML methods like KNN, as demonstrated in studies by [48], [49]. Additionally, studies such as those by [11] and [12] have employed ML methods like RF, DT, and SVM to predict the final area burned and fire severity, highlighting the effectiveness of these models in handling complex wildfire data. However, these ML methods often face challenges related to parameter tuning, computational demands, and limitations in handling large, multivariate datasets.

On the other hand, DL methods have emerged as powerful tools for burned area detection and fire severity mapping, particularly in scenarios involving large and complex datasets. DL architectures, such as CNNs and semantic segmentation networks like U-Net [50], Fast-SCNN, and DeepLabv3+ [51], have shown remarkable capabilities in automatically capturing object features at multiple scales and providing detailed, accurate, and bias-free burned area maps [52]. Recent studies have demonstrated the superiority of DL models over traditional ML approaches, particularly in cases involving compact burned scars and heterogeneous landscapes. For instance, [20] applied a deep neural network (DNN) for wildfire classification across Alaska using MODIS variables, achieving better accuracy compared to traditional methods. Additionally, DL models have been successfully applied to cross-sensor multispectral data from Sentinel-2 and Landsat-8, offering high accuracy in different local climate zones [53]. While DL models excel in capturing spatial details and contextual information, they require large datasets and significant computational resources, making them more suitable for large-scale, automated mapping tasks. Overall, DL methods represent a significant advancement in burned area and fire severity mapping, enabling precise and efficient post-fire assessments that are critical for understanding the ecological and economic impacts of wildfires.

VI. CONCLUSION

This paper reviews significant advancements in machine learning (ML) and deep learning (DL) technologies across the stages of wildfire management. As shown in Table I, ML and DL have surpassed traditional methods, offering enhanced accuracy and faster response times in pre-fire fuel type classification, active-fire detection, and post-fire damage assessment.

In pre-fire management, ML improves classification accuracy by integrating diverse data sources, while DL excels in feature extraction. Active-fire management benefits from DL models like CNNs and vision transformers, which provide rapid and accurate fire detection. In the post-fire phase, these technologies enable detailed assessments of fire severity and burned areas, significantly improving over traditional survey methods.

Future efforts should focus on increasing the adaptability of these models to different environments, reducing computational costs, and integrating real-time data to enhance responsiveness. By advancing ML and DL capabilities, this research supports more effective wildfire management and contributes to the resilience of infrastructure and communities against future fire threats.

REFERENCES

[1] C. W. F. I. System, "Fire weather maps: Fire weather index (fwi)," https://cwfis.cfs.nrcan.gc.ca/maps/fw?type=fwi, 2024.

[2] W. J. Bond and J. E. Keeley, "Fire as a global 'herbivore': the ecology and evolution of flammable ecosystems," Trends in ecology & evolution, vol. 20, no. 7, pp. 387–394, 2005.

[3] A. Al-Najjar, M. Amini, S. Rajan, and J. R. Green, "Identifying areas of high-risk vegetation encroachment on electrical powerlines using mobile and airborne laser scanned point clouds," IEEE Sensors Journal, vol. 24, no. 14, pp. 22 129–22 143, 2024.

[4] S. W. Taylor, M. E. Alexander, and R. Pike, Field Guide to the Canadian forest fire behaviour prediction (FBP) system. Canadian Forest Service, Northern Forestry Centre Edmonton, Alberta, Canada, 1997, vol. 11.

[5] F. A. Albini, Estimating wildfire behavior and effects. Department of Agriculture, Forest Service, Intermountain Forest and Range . . . , 1976, vol. 30.

[6] B. C. Arrue, A. Ollero, and J. M. De Dios, "An intelligent system for false alarm reduction in infrared forest-fire detection," IEEE Intelligent Systems and their Applications, vol. 15, no. 3, pp. 64–73, 2000.

[7] J. He, T. V. Loboda, L. Jenkins, and D. Chen, "Mapping fractional cover of major fuel type components across alaskan tundra," Remote Sensing of Environment, vol. 232, p. 111324, 2019.

[8] C. Cleve, M. Kelly, F. R. Kearns, and M. Moritz, "Classification of the wildland–urban interface: A comparison of pixel-and object-based classifications using high-resolution aerial photography," Computers, Environment and Urban Systems, vol. 32, no. 4, pp. 317–326, 2008.

[9] J. Zhao, Z. Zhang, S. Han, C. Qu, Z. Yuan, and D. Zhang, "Svm based forest fire detection using static and dynamic features," Computer Science and Information Systems, vol. 8, no. 3, pp. 821–841, 2011.

[10] M. Elia, M. D'Este, D. Ascoli, V. Giannico, G. Spano, A. Ganga, G. Colangelo, R. Lafortezza, and G. Sanesi, "Estimating the probability of wildfire occurrence in mediterranean landscapes using artificial neural networks," Environmental Impact Assessment Review, vol. 85, p. 106474, 2020.

[11] P. Cortez and A. d. J. R. Morais, "A data mining approach to predict forest fires using meteorological data," unkn, 2007.

[12] H. S. Zald and C. J. Dunn, "Severe fire weather and intensive forest management increase fire severity in a multi-ownership landscape," Ecological Applications, vol. 28, no. 4, pp. 1068–1080, 2018.

[13] K. Al-Rawi, J. Casanova, and A. Calle, "Burned area mapping system and fire detection system, based on neural networks and noaa-avhrr imagery," International Journal of Remote Sensing, vol. 22, no. 10, pp. 2015–2032, 2001.

[14] R. Pu and P. Gong, "Determination of burnt scars using logistic regression and neural network techniques from a single post-fire landsat 7 etm+ image," Photogrammetric Engineering & Remote Sensing, vol. 70, no. 7, pp. 841–850, 2004.

[15] A. Abdollahi and B. Pradhan, "Urban vegetation mapping from aerial imagery using explainable ai (xai)," Sensors, vol. 21, no. 14, p. 4738, 2021.

[16] T. Kattenborn, J. Leitloff, F. Schiefer, and S. Hinz, "Review on convolutional neural networks (cnn) in vegetation remote sensing," ISPRS journal of photogrammetry and remote sensing, vol. 173, pp. 24–49, 2021.

[17] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," nature, vol. 521, no. 7553, pp. 436–444, 2015.

[18] B. Zhang, W. Wei, B. He, and C. Guo, "Early wildfire smoke detection based on improved codebook model and convolutional neural networks," in Tenth International Conference on Digital Image Processing (ICDIP 2018), vol. 10806. SPIE, 2018, pp. 1624–1631.

[19] Y. Cao, F. Yang, Q. Tang, and X. Lu, "An attention enhanced bidirectional lstm for early forest fire smoke recognition," IEEE Access, vol. 7, pp. 154 732–154 742, 2019.

[20] Z. Langford, J. Kumar, and F. Hoffman, "Wildfire mapping in interior alaska using deep neural networks on imbalanced datasets," in 2018 IEEE International Conference on Data Mining Workshops (ICDMW). IEEE, 2018, pp. 770–778.

[21] L. Knopp, M. Wieland, M. Rattich, and S. Martinis, "A deep learning ¨ approach for burned area segmentation with sentinel-2 data," Remote Sensing, vol. 12, no. 15, p. 2422, 2020.

[22] R. Hagmann, P. Hessburg, S. Prichard, N. Povak, P. Brown, P. Fule,´ R. Keane, E. Knapp, J. Lydersen, K. Metlen et al., "Evidence for widespread changes in the structure, composition, and fire regimes of western north american forests," Ecological Applications, vol. 31, no. 8, p. e02431, 2021.

[23] S. J. Prichard, P. F. Hessburg, R. K. Hagmann, N. A. Povak, S. Z. Dobrowski, M. D. Hurteau, V. R. Kane, R. E. Keane, L. N. Kobziar, C. A. Kolden et al., "Adapting western north american forests to climate change and wildfires: 10 common questions," Ecological applications, vol. 31, no. 8, p. e02433, 2021.

[24] E. Marino, P. Ranz, J. L. Tome, M. ´ A. Noriega, J. Esteban, and ´ J. Madrigal, "Generation of high-resolution fuel model maps from discrete airborne laser scanner and landsat-8 oli: A low-cost and highly updated methodology for large areas," Remote Sensing of Environment, vol. 187, pp. 267–280, 2016.

[25] L. Fogarty, H. Pearce, W. Catchpole, and M. Alexander, "Adoption vs. adaptation: lessons from applying the canadian forest fire danger rating system in new zealand," in Proceedings, 3rd International Conference on Forest Fire Research and 14th Fire and Forest Meteorology Conference, Luso, Coimbra, Portugal, 1998, pp. 1011–1028. [26] L. A. Arroyo, C. Pascual, and J. A. Manzanera, "Fire models and methods to map fuel types: The role of remote sensing," Forest ecology and management, vol. 256, no. 6, pp. 1239–1252, 2008.

[27] Q. Yu, P. Gong, N. Clinton, G. Biging, M. Kelly, and D. Schirokauer, "Object-based detailed vegetation classification with airborne high spatial resolution remote sensing imagery," Photogrammetric Engineering & Remote Sensing, vol. 72, no. 7, pp. 799–811, 2006.

[28] A. Alonso-Benito, L. A. Arroyo, M. Arbelo, and P. Hernandez-Leal, ´ "Fusion of worldview-2 and lidar data to map fuel types in the canary islands," Remote Sensing, vol. 8, no. 8, p. 669, 2016.

[29] A. Puissant, S. Rougier, and A. Stumpf, "Object-oriented mapping of urban trees using random forest classifiers," International Journal of Applied Earth Observation and Geoinformation, vol. 26, pp. 235–245, 2014.

[30] Q. Guo, S. Jin, M. Li, Q. Yang, K. Xu, Y. Ju, J. Zhang, J. Xuan, J. Liu, Y. Su et al., "Application of deep learning in ecological resource research: Theories, methods, and challenges," Science China Earth Sciences, vol. 63, pp. 1457–1474, 2020.

[31] A. Vali, S. Comai, and M. Matteucci, "Deep learning for land use and land cover classification based on hyperspectral and multispectral earth observation data: A review," Remote Sensing, vol. 12, no. 15, p. 2495, 2020.

[32] J. M. Bioucas-Dias, A. Plaza, N. Dobigeon, M. Parente, Q. Du, P. Gader, and J. Chanussot, "Hyperspectral unmixing overview: Geometrical, statistical, and sparse regression-based approaches," IEEE journal of selected topics in applied earth observations and remote sensing, vol. 5, no. 2, pp. 354–379, 2012.
[33] Q.-x. Zhang, G.-h. Lin, Y.-m. Zhang, G. Xu, and J.-j. Wang, "Wildland forest fire smoke detection based on faster r-cnn using synthetic smoke images," Procedia engineering, vol. 211, pp. 441–446, 2018.
[34] J. Yuan, L. Wang, P. Wu, C. Gao, and L. Sun, "Detection of wildfires along transmission lines using deep time and space features," Pattern Recognition and Image Analysis, vol. 28, pp. 805–812, 2018.
[35] H. Soliman, K. Sudan, and A. Mishra, "A smart forest-fire early detection sensory system: Another approach of utilizing wireless sensor and neural networks," in SENSORS, 2010 IEEE. IEEE, 2010, pp. 1900– 1904.
[36] Y. O. Sayad, H. Mousannif, and H. Al Moatassime, "Predictive modeling of wildfires: A new dataset and machine learning approach," Fire safety journal, vol. 104, pp. 130–146, 2019.
[37] L. Collins, P. Griffioen, G. Newell, and A. Mellor, "The utility of random forests for wildfire severity mapping," Remote sensing of Environment, vol. 216, pp. 374–384, 2018.
[38] A. Rezaei Barzani, P. Pahlavani, and O. Ghorbanzadeh, "Ensembling of decision trees, knn, and logistic regression with soft-voting method for wildfire susceptibility mapping," ISPRS Annals of the Photogrammetry, Remote Sensing and Spatial Information Sciences, vol. 10, pp. 647–652, 2023.
[39] A. Jaafari, E. K. Zenner, and B. T. Pham, "Wildfire spatial pattern analysis in the zagros mountains, iran: A comparative study of decision tree based classifiers," Ecological informatics, vol. 43, pp. 200–211, 2018.
[40] Z. Zhou, Y. Shi, Z. Gao, and S. Li, "Wildfire smoke detection based on local extremal region segmentation and surveillance," Fire Safety Journal, vol. 85, pp. 50–58, 2016. [41] A. Jaafari, E. K. Zenner, M. Panahi, and H. Shahabi, "Hybrid artificial intelligence models based on a neuro-fuzzy system and metaheuristic optimization algorithms for spatial prediction of wildfire probability," Agricultural and forest meteorology, vol. 266, pp. 198–207, 2019.
[42] A. Cordoba, R. Vilar, A. Lavrov, A. Utkin, and A. Fernandes, "Multiobjective optimisation of lidar parameters for forest-fire detection on the 7 basis of a genetic algorithm," Optics & Laser Technology, vol. 36, no. 5, pp. 393–400, 2004.
[43] X. Li, Z. Chen, Q. M. J. Wu, and C. Liu, "3d parallel fully convolutional networks for real-time video wildfire smoke detection," IEEE Transactions on Circuits and Systems for Video Technology, vol. 30, no. 1, pp. 89–103, 2020.
[44] D. Alexandrov, E. Pertseva, I. Berman, I. Pantiukhin, and A. Kapitonov, "Analysis of machine learning methods for wildfire security monitoring with an unmanned aerial vehicles," in 2019 24th conference of open innovations association (FRUCT). IEEE, 2019, pp. 3–9.
[45] R. Ghali, M. A. Akhloufi, and W. S. Mseddi, "Deep learning and transformer approaches for uav-based wildfire detection and segmentation," Sensors, vol. 22, no. 5, p. 1977, 2022.
[46] X. Wang, Z. Pan, H. Gao, N. He, and T. Gao, "An efficient model for real-time wildfire detection in complex scenarios based on multi-head attention mechanism," Journal of Real-Time Image Processing, vol. 20, no. 4, p. 66, 2023.
[47] P. Jain, S. C. Coogan, S. G. Subramanian, M. Crowley, S. Taylor, and M. D. Flannigan, "A review of machine learning applications in wildfire science and management," Environmental Reviews, vol. 28, no. 4, pp. 478–505, 2020.
[48] O. Zammit, X. Descombes, and J. Zerubia, "Burnt area mapping using support vector machines," Forest Ecology and Management, vol. 234, no. 1, p. S240, 2006.
[49] E. Dragozi, I. Gitas, D. Stavrakoudis, and J. Theocharis, "A performance evaluation of support vector machines and the nearest neighbor classifier in classifying image objects for burned area mapping," Advances in Remote Sensing and GIS applications in Forest Fire Management From local to global assessments, p. 87, 2011. [50] O. Ronneberger, P. Fischer, and T. Brox, "U-net: Convolutional networks for biomedical image segmentation," in Medical image computing and computer-assisted intervention–MICCAI 2015: 18th international conference, Munich, Germany, October 5-9, 2015, proceedings, part III 18. Springer, 2015, pp. 234–241.
[51] L.-C. Chen, Y. Zhu, G. Papandreou, F. Schroff, and H. Adam, "Encoderdecoder with atrous separable convolution for semantic image segmentation," in Proceedings of the European conference on computer vision (ECCV), 2018, pp. 801–818.
[52] X. Hu, P. Zhang, and Y. Ban, "Large-scale burn severity mapping in multispectral imagery using deep semantic segmentation models," ISPRS Journal of Photogrammetry and Remote Sensing, vol. 196, pp. 228–240, 2023.
[53] X. Hu, Y. Ban, and A. Nascetti, "Uni-temporal multispectral imagery for burned area mapping with deep learning," Remote Sensing, vol. 13, no. 8, p. 1509, 2021.

May 2024 solar storm Observed by Health Canada's environmental radiation monitoring detectors

Tamara R. Koletic

ABSTRACT

On May 10th, 2024, Health Canada's Fixed Point Surveillance (FPS) network detected a Forbush decrease event, evidence of the occurrence of a strong solar storm. Correcting the cosmic count rates for pressure and temperature effects, the rescaled counts follow the same trend observed in global muon and neutron detections. Additionally, the onset and maximum disturbance time of the event match those measured by collocated geomagnetic observatories. This study demonstrates that the FPS network can be used for real-time space weather monitoring.

INTRODUCTION

Health Canada's Fixed-Point Surveillance (FPS) network is a nation wide system of detectors developed to monitor both anthropogenic and natural radiation sources. The network consists of over eighty detectors, spanning from Resolute, NT in the north to Southern Ontario. As a part of a network upgrade, a fleet of five RS252d detectors were installed at the Natural Research Council of Canada (NRCan) near Anderson Road, Ottawa, in July 2023. The RS252d are sodium iodine spectrometers manufactured by Radiation Solutions Incorporate (RSI). The purpose of deploying the five detectors was to test a new gain stabilization algorithm. Due to the detectors' close proximity, the combined signal of the fleet offers a better cosmic ray response with improved statistical uncertainty.

This report analyzes the response of these detectors to the strong solar flare activity and coronal mass ejections (CME) during May 7-14, 2024. CMEs are highly energetic particles/plasma and magnetic fields ejected from the sun during solar activity. Though cloud cover in Ottawa prevented residents from witnessing the brilliant display of aurora, the Anderson fleet captured the characteristic Forbush decrease caused by the solar storm. The decrease feature is a result of the suppression of incident galactic cosmic rays by the magnetic field of the charged CME. The lack of cosmic rays shows up as a rapid decrease in the particle counts recorded by ground level detectors. The timings of this event detected by the FPS network match muon and neutron results available from international public databases.

ANDERSON ROAD EXPERIMENTAL SITE

The Anderson Road detector fleet is a group of five detectors (6029, 6031, 6037, 6038, and 6041) located in the back compound of one of NRCan's buildings in Ottawa, ON. These detectors return nearly identical results due to their proximity to each other (figure 1). The thallium doped sodium iodide (NaI(Tl)) detectors consist of an RS252d spectrometer produced by RSI and a temperature sensor. RS252d measures terrestrial radiation in 1023 channels from 0-3 MeV, with one cosmic channel for counts above 3 MeV. Each detector is programed with one of three different gain configuration methods; fixed gain, spectral-based stabilization, and temperature-controlled gain. Gain shifts caused by environmental factors, primarily ambient temperature, generate drifts in the gamma-ray spectrum (Bu et al., 2018). The purpose of the fleet is to analyze the three configuration methods and keep the dose bias from gain drift lower than 10%. RS252d records multiple parameters including total Air Kerma rate, the Air Kerma rates of Xe-135, Xe-133, and Ar-41, gain, temperature, and cosmic count rate.

Figure 1: Anderson fleet in back compound of the NRCan building. (credit: Colin Vant)

MAY SOLAR STORM

Solar activities, including CMEs, solar flares, and solar energetic particles, can disrupt the geomagnetic and ionospheric conditions and potentially alter background radiation levels. This affects ground-based communications, infrastructure, and navigation networks and may pose a biological hazard to astronauts and aircraft personnel (Liu et al., 2023).

The May solar storm started with the release of two strong solar flares on May 7th. Over the course of the next few days, NASA detected many more solar flares and seven CMEs (NASA and Interrante (Ed.), 2024). From May 7th to 11th, eight of these flares were catalogued as X-class with the strongest during this period classified as an X5.8 on May 10th, shown in figure 2 (NASA and Interrante (Ed.), 2024). On May 14th this same solar region released an X8.7 flare, the most powerful flare recorded during this solar cycle (NASA and Interrante (Ed.), 2024). We are currently at the peak of solar cycle 25, the onset of which began in 2019 (Dobrijevic , 2022). The CMEs reached Earth on May 10th, causing a G5 level geomagnetic storm, resulting in powerful aurorae visible around the world and the lowest-latitude aurora sightings recorded in the past five centuries (NASA and Interrante (Ed.), 2024). The aurorae were captured by professional and amateur photographers alike, as depicted in the two images in figure 3, one taken in southwest British Colombia by NASA/ Mara Johnson-Groh (left) and the other by Gunjan Sinha near Saskatoon (right) (Hansen, 2024).

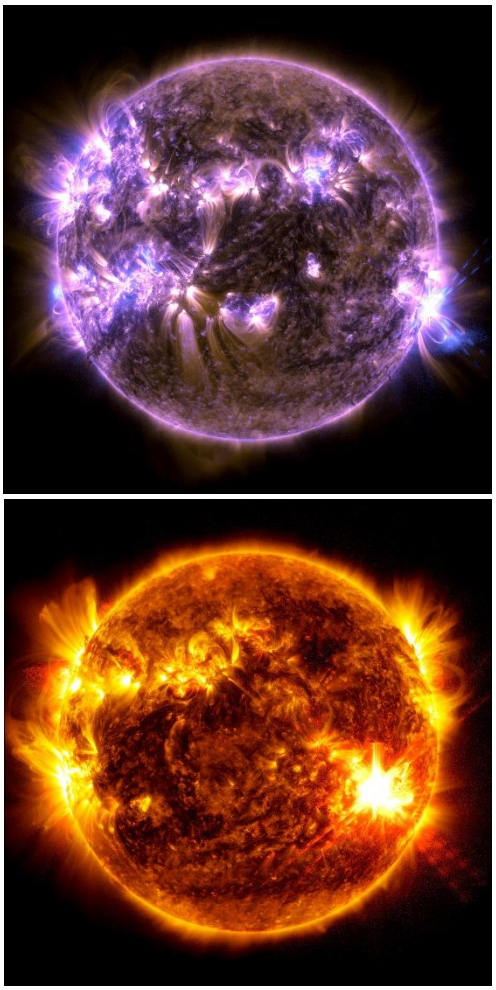

Figure 2: Solar flare captured by NASA. Image description: (Top) X5.8 solar flare captured by NASA's Solar Dynamics Observatory on May 10, 2024 at 9:23 pm. (Bottom) X1.7 solar flare peaking at 10:09 p.m. EDT on May 13, 2024. These images depict a subset of extreme UV light that illustrate the extremely hot material in the flares. (NASA's Goddard Space Flight Center, 2024).

Figure 3: Examples of aurora captured on May 10, 2024. Image description: A coronal aurora taken in southwest British Columbia by NASA/Mara Johnson-Groh (top) (NASA and Interrante (Ed.), 2024) and an aurora captured by Gunjan Sinha near Saskatoon (bottom) on May 11, 2024 (Hansen, 2024).

Data Analysis

The average cosmic counts from four of the Anderson detectors were averaged from May 1st to June 3rd, encompassing the entire duration of the solar event. Data from the fixed gain detector was removed from the average because it does not correctly respond to counts above 3 MeV. The cosmic counts for the four detectors were pressure and temperature corrected using hourly Environment Canada weather data from the Ottawa International Airport station. The method for pressure correction in this analysis was used in the early Forbush decrease studies in 2023 (Liu et al., 2023), initially from (Malandraki and Crosby, 2018).

The relationship between the atmospheric pressure and the recorded counts is expressed as:

$$n = n_0 e^{\beta(p-p_0)}$$

Where β is the barometric coefficient found from the slope of the linear regression of the cosmic count variation and pressure variation. The variables n_0 and p_0 are the corrected cosmic count and reference pressure, respectively. In this analysis, the coefficient β was estimated as -2.34 ± 0.001 %/kPa. In the 2023 Forbush decrease study, the coefficient was calculated at -2.58 ± 0.001 %/kPa. The temperature corrections were calculated using the same method, replacing the pressure values with temperature and the raw cosmic count with the pressure corrected results.

Hourly pressure- and efficiency-corrected neutron data was downloaded from the Neutron Monitor Database (nmdb.eu/nest/) from the NAIN station, the closest neutron station to Ottawa located in Nain, NL. Vertical muon data was taken from the 1-hour Yakutsk station (07 m w.e. telescope), located in Yakutsk, Russia from the ysn Cosmic Ray Database (IKFIA SB RAS "Cosmic Ray Database" (ysn.ru)). Ottawa hourly geomagnetic indices were downloaded from Natural Resources Canada and Kp indices were provided by NRCan. In future studies, geomagnetic data can be downloaded from the International Real-time Magnetic Observatory Network (INTERMAGNET) at https://intermagnet.org/. The neutron, muon, and the data from the detectors at the Anderson Road site were scaled using the respective mean count values from April 7th to 14th, a week before the solar event.

Results and Discussion

Evidence of the May event captured by various measurements

The temporal profile of the Anderson Road detector's response to the May solar storm is shown in figure 4. The rapid decrease, reaching a minimum on May 10, 2024, at 23:00 UTC, is evidence of the Forbush decrease caused by this event. NRCan recorded the onset time of the geomagnetic field disturbance at 18:00 UTC on May 10th, matching the onset time of the Forbush decrease observed with the Anderson Road

detectors. The maximum geomagnetic and Kp indices were found to align with the Forbush decrease minimum at this time. The Kp index has a slightly shifted onset time. This could be explained by the way this index is calculated; it is the averaged magnetic field variation around the world in 3 hr resolution. Also, the Anderson Road site cosmic counts match the trends of the neutron and muon data as depicted in this figure. However, the amplitude of the lowest dip in the cosmic count is about 50% less than that of the neutron results, indicating that the FPS network works more similarly to a muon detector than a neutron detector. These relative amplitude levels are consistent with the findings of Liu et al., 2023.

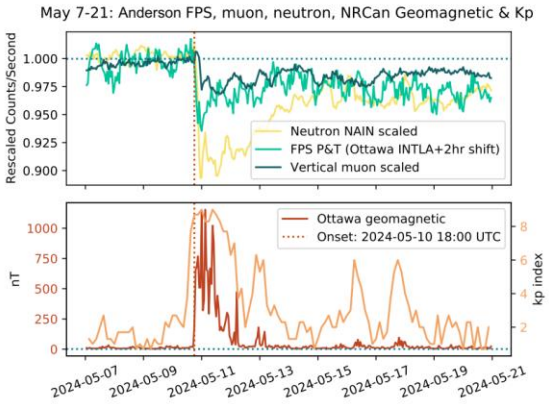

Figure 4: NRCan magnetic disturbance and Kp index plotted alongside Anderson, muon, and neutron data

TEMPERATURE CORRECTION

It has long been known that meteorological conditions such as atmospheric pressure and temperature have a large impact on the cosmic ray flux observed at a location (De Mendonça et al., 2016). In this work, the meteorological data measured from the Ottawa International Airport (INTLA) weather station were used to correct these effects on the Anderson Road detector measurements.

Additionally, each Anderson Road detector is outfitted with an Advanced Digital Spectrometer Temperature (ADST) sensor inside the electronic box. These temperatures are on average 7 °C higher than the INTLA data, which could be due to sealing effects and electronic heating inside the box. Further analysis revealed the phase of the ADST data was slightly shifted by +2 hours compared to the Ottawa airport temperatures.

In studying the temperature effects on cosmic ray flux, it is acknowledged that the ground level temperature variation is only a way to represent the change in temperature conditions in the upper atmosphere where cosmic muons are typically generated. Bearing this in mind, a few tests have been conducted by using different temperature datasets to correct the cosmic ray data in the Anderson Road detectors. The figure 5-top shows FPS Anderson counts corrected for pressure and temperature effects using the airport data, while the right uses airport pressure data and ADST temperature data from detector 6041. The comparison suggests a smoother or more precise trend from the ADST corrected counts. Here the difference between using the temperature from station 6041 verus an average of 4 stations is negligible.

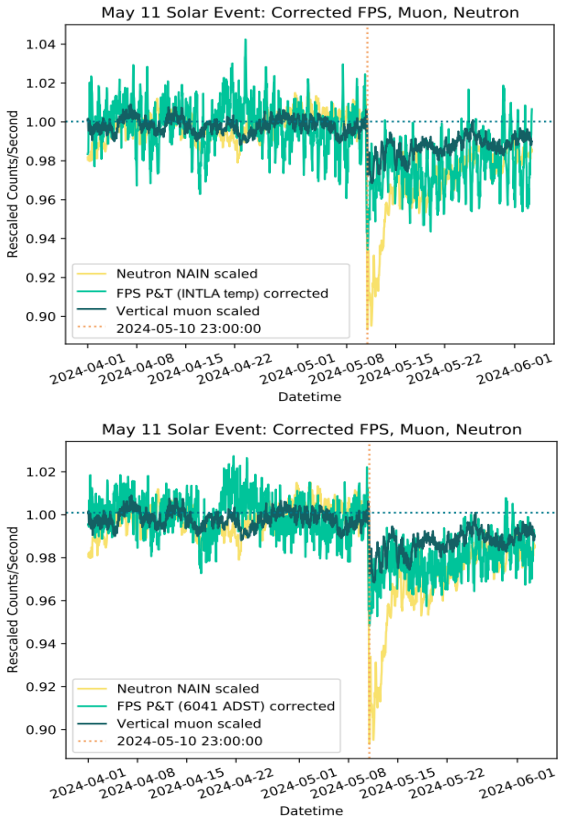

Figure 5: ADST and non-shifted corrected Anderson cosmic counts

Figure 6-top shows the phase similarity between ADST data and 2-hr shifted INTLA temperature data, whereas the right shows the corrected Anderson count profile using the shifted temperatures. In this profile, the daily oscillations were smeared to certain extent when compared to non-shifted results in figure 5-top, but they did not reach the smooth level found in figure 5-bottom.

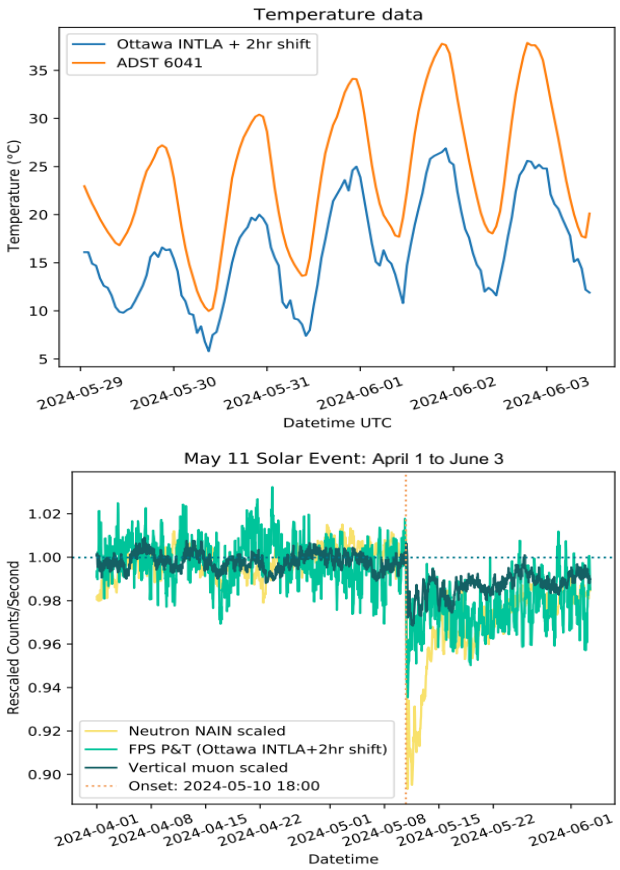

Figure 6: Anderson corrected counts using phase shifted Ottawa airport temperature data.

DAILY CYCLES

After the Forbush decrease dip, the oscillations in the corrected cosmic counts only include the higher (short-term) frequency, with the lower (long-term) frequency oscillations appearing prior to the dip onset. An analysis of the Anderson Road detector data over a longer period shows this trend more clearly. Figure 7 shows pressure-only corrected cosmic counts from April 1st to June 3rd, featuring the high and low frequencies.

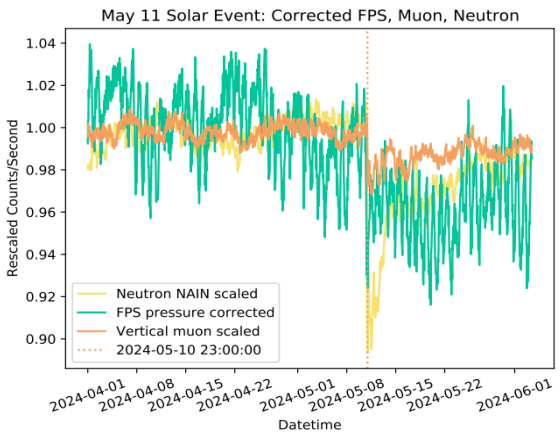

Figure 7: Anderson pressure-only corrected counts showing the high and low frequency trends

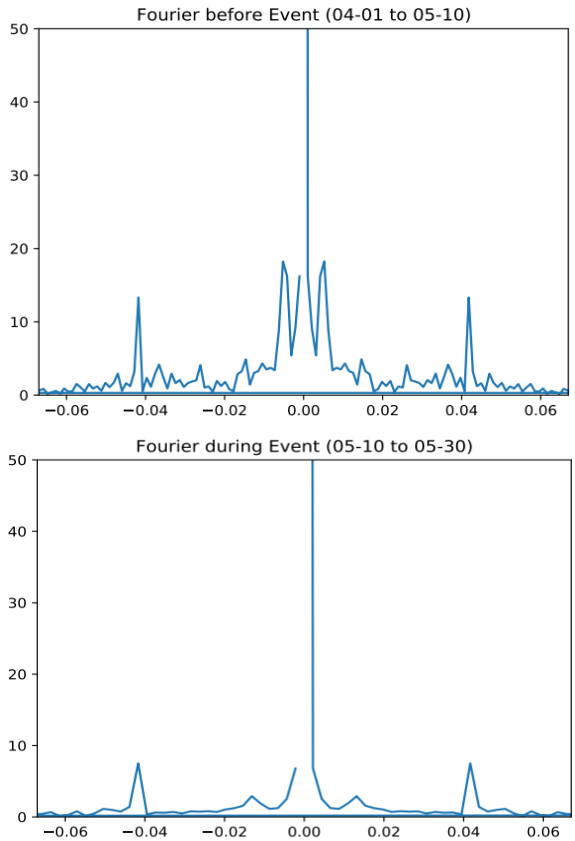

Figure 8: Fourier transform of corrected Anderson cosmic counts before and during solar event

The graphs in figure 8 show the Fourier transform of the Anderson pressure and temperature corrected data before and during the event. The Fourier transform from April 1st to May 10th picks up both frequencies, the high frequency spike at 0.0421 and the low spike around 0.00570 which correspond to periods of 23.75 hours (~1 day) and 7.31 days (~ 1 week) respectively. However, the low frequency is missing during the event (figure 8-bottom) which matches the trend observed in figure 7.

The cause of the high frequency (i.e., daily oscillations) is not fully understood, neither the corresponding corrections on them. A check of other FPS stations around Health Canada show these oscillations, though to a lesser extent. One possibility is that the high frequency is caused by incoming cosmic rays in the high energy domain which are less susceptible to geomagnetic and environmental variation. In this event, the shielding effect of the magnetic solar wind largely blocks the low energy cosmic rays, leaving the surviving ones dominated by high energy cosmic rays. Furthermore, the Earth's rotation may also play a role in the daily variation. Another possibility is the high frequency originates from high-energy terrestrial sources.

An investigation into the Anderson Road detector data prior to the May solar event and May 2023 data from a different Ottawa detector also show this high frequency, making this explanation more likely. The cycle could be caused by the diurnal fluctuation of radon emissions whose progeny can produce gamma-rays above 3 MeV (EL-Hussein, 2001). Another reason could be thermal neutrons, the levels of which are affected at ground level by environmental conditions and have been observed to fluctuate diurnally (Stenkin, 2021). Further investigation into the cause of the cycle is ongoing.

As of May 31, 2024, high solar activity is ongoing in the same region that released the powerful flares (Sutherland, 2024). Consequently, the muon, neutron, and cosmic counts have not recovered to levels prior to the event onset.

Conclusion

During the May solar storm, a large Forbush decrease event was detected by the RS252d detectors located at the NRCan facility on Anderson Road, Ottawa. The rescaled cosmic radiation counts/s in the FPS network follow the same trends found in other radiation (i.e., muon and neutron) monitoring systems. More importantly, the FPS responses match the onset and maximum disturbance times of the collocated NRCan's geomagnetic temporal profiles. This case study is another example showing that Health Canada's FPS network can be used for real-time space weather monitoring. Its data offers a different and complementary perspective on space weather events than NRCan's magnetic data, but with a comparable response profile.

Acknowledgements

Thanks are due to Dr. Chuanlei Liu and Dr. Kurt Ungar from Health Canada for assistance with the data analysis and contributions to this article, as well as to all team members in the Anderson project. I thank Dr. Robyn Fiori from NRCan for providing the magnetic index data. I also acknowledge the Neutron Monitor Database and the Global Muon Detector Network for providing neutron and muon data.

About the Author

Tamara R. Koletic is a Radiation Officer affiliated with the Radiation Protection Bureau of Health Canada. She received her bachelor's degree in physics and astronomy from the University of Waterloo and will start her master's degree at McMaster University in September 2024. Her areas of research at the Radiation Protection Bureau include cosmic radiation, terrestrial radiation, and space weather.

References

[1] Bu, M., Murray, A. S., Kook, M., Helsted, L. M., Buylaert, J.-P., & Thomsen, K. J. (2018). Characterisation of scintillator-based gamma spectrometers for determination of sample dose rate in OSL dating applications. *Radiation Measurements*, *120*, 253–259. https://doi.org/10.1016/j.radmeas.2018.07.003

[2] De Mendonça, R. R., Braga, C. R., Echer, E., Dal Lago, A., Munakata, K., Kuwabara, T., Kozai, M., Kato, C., Rockenbach, M., Schuch, N. J., Al Jassar, H. K., Sharma, M. M., Tokumaru, M., Duldig, M. L., Humble, J. E., Evenson, P., & Sabbah, I. (2016). The temperature effect in secondary cosmic rays (muons) observed at the ground: Analysis of the Global Muon Detector Network Data. *The Astrophysical Journal*, *830*(2). https://doi.org/10.3847/0004-637x/830/2/88

[3] Dobrijevic, D. (2022, April 25). *Solar cycle: What is it and why does it matter?*. Space.com. https://www.space.com/solar-cycle-frequency-prediction-facts

[4] EL-Hussein, A., Mohamemed, A., Abd EL-Hady, M., Ahmed, A. A., Ali, A. E., & Barakat, A. (2001). Diurnal and seasonal variation of short-lived radon progeny concentration and atmospheric temporal variations of 210PB and 7be in Egypt. *Atmospheric Environment*, *35*(25), 4305–4313. https://doi.org/10.1016/s1352-2310(01)00206-0

[5] Environment and Climate Change Canada. *Historical Data – Ottawa INTL A.* Station Results - Historical Data - Climate - Environment and Climate Change Canada (weather.gc.ca)

[6] Hansen, K. (2024, May 15). *Citizen Scientists Capture Brilliant Photos of the Aurora*. Earth Matters - Earth Observatory. https://earthobservatory.nasa.gov/blogs/earthmatters/2024/05/15/citizen-scientists-capture-brilliant-photos-of-the-aurora/

[7] Liu, C., Koletic, T., Ungar, K., Trichtchenko, L., & Sinclair, L. (2023). Space weather monitoring with Health Canada's Terrestrial Radiation Monitoring Network. *Advances in Space Research*, *72*(12), 5607–5625. https://doi.org/10.1016/j.asr.2023.06.018

[8] Malandraki, O. E., & Crosby, N. (2018). *Solar particle radiation storms forecasting and analysis: The Hesperia Horizon 2020 project and beyond* (Vol. 444). Springer.

[9] NASA's Goddard Space Flight Center, Hatfield, M. S., & Weissinger, S. (2024, May 14). *Continued Strong Solar Flare Activity: May 10-14, 2024*. NASA. https://svs.gsfc.nasa.gov/14589

[10] NASA, Interrante, A. (Ed.). (2024, May 16). *How NASA tracked the most intense solar storm in decades - NASA science*. NASA. https://science.nasa.gov/science-research/heliophysics/how-nasa-tracked-the-most-intense-solar-storm-in-decades/

[11] Neutron Monitor Data Base. nmdb.eu/nest/ Starodubstev, S. A. *The 1-hour Yakutsk muon telescope data (07 m w.e.).* Cosmic Ray Database. ysn.ru/ipm/yktMT07/

[12] Stenkin, Yu. V. (2021). Study of Environmental Thermal Neutron Fluxes: From EAS to geophysics. *Physics of Atomic Nuclei*, *84*(6), 929–933. https://doi.org/10.1134/s1063778821130354

[13] Sutherland, S. (2024, May 31). *Look up! bright auroras possible across Canada Friday night*. The Weather Network. https://www.theweathernetwork.com/en/news/science/space/solar-flare-and-solar-storm-may-spark-auroras-across-canada-friday-night

Resilience in Leadership:

Personal and Organizational Requirements and Effects of Building Resiliency

Valerie A.R. Keyes, CD, MA, MSL

Experience shows that resilience in leadership plays a major role in the attainment of personal, professional and organisational goals as well as being an essential part of leadership responsibility and accountability. The factors of resilience can combine to be a powerful force for success for individuals, teams, organisations and ultimately communities. However, without personal resilience, organisations cannot support resilient infrastructure, as it rapidly becomes irrelevant to the attainment of goals and ambitions if the people factor is not regarded first. This paper examines the fundamental factors that build resilience at all levels of an organisation, from the individual to the leader, and thence to the whole organisation. It concludes with steps that will assist leaders to become more resilient, thereby building better and stronger organisations that can withstand challenges and adversities.

What do we mean by 'resilience', and why is it so important? Resilience may be defined as the continued pursuit of goals despite the adversity and challenges that individuals face on a daily basis, regardless as to whether they are serving as team leaders or team members, and equally regardless as to whether they are faced with the inevitability of adversity that exists in everyone's personal lives and professional careers.[1]

Some experts refer to 'resonant' leaders and organisations,[2] while other authors emphasise the compassionate or human aspects of leadership that enable organisations to function effectively[3]. That said, what it all comes down to is that leaders at all levels have to develop – and display – the softer or more human skills that are included in the concept of *Emotional Intelligence*. The first point to understand is that superior cognitive abilities don't necessarily contribute to the creation of resilient organisations, but must be tempered by the addition of the skills that support and encourage employees without losing sight of the corporate, team or individual goals.[4] The overwhelming information overload, with which we must all cope these days, can easily result in cognitive stagnation, stress and frustration, seriously undermining the whole ethos and attempts of the

---

[1] There are obviously many definitions of resilience. My preferred one produced here is that of Daniel Goleman and Warren Bennis whose decades long research into leadership requirements and sustainability is widely accepted and respected. See particularly Warren Bennis, James O'Toole, and Daniel Goleman. *Transparency: How Leaders Create a Culture of Candor*. Jossey Bass, 2008.

[2] See, for example, Anne McKee, Richard Boyatzis, and Frances Johnston. *Becoming a Resonant Leader: Develop Your Emotional Intelligence, Renew Your Relationships, Sustain Your Effectiveness*. Boston: Harvard Business Review Press, 2008. The research and education undertaken leadership in recent years by the Teleos Institute under Dr Frances Johnston's expands on the concept of resonant leadership.

[3] Rasmus Hougaard and Jacqueline Carter. *Compassionate Leadership: How to Do Hard Things in a Human Way.* Boston, Mass.: Harvard Business Review Press, 2022.

[4] Daniel Goleman. What Makes a Leader?" *Harvard Business Review*. January 2004. pp. 4-12; and Goleman, *Emotional Intelligence: Why It Can Matter More than IQ*. New York: Bantam Books, 1995. pp.117-20.

organisation and its members to make rational decisions.[5]

Clearly, it is equally important for organisations to be resilient and to display this resilience, given the adversities that industries and businesses currently face, such as cyberattacks, physical terrorist threats, supply chain disruptions, and so on. Organisations must be sustainable and be able to show results both internally and externally. However, without building resilient organisations, no leaders, managers or employees can hope to develop, mature, or create success or value for all concerned.

Resilience must therefore be built into our individual, corporate and collective mindsets in order to enable us to react swiftly to challenges; absorb the stresses these challenges can cause without losing sight of our goals; and recover or reinvent ourselves and our organisations following any sort of a blow or injury. This is particularly important when we see the rapidly changing workplaces, methodologies of work and therefore interpersonal communications and the creation of more remote or distant work relationships, including where staffs rarely see their immediate superiors, let alone the organisational leaders at the highest levels.[6]

Personal Resilience

As a first step, we need to understand the factors that build resilience in individuals as well as organisations. On a personal level, these can include:[7]

Emotional regulation – The ability to maintain an even keel in the face of even the most threatening circumstances is difficult but essential in being able to carry assigned tasks and roles to successful conclusions.

Impulse control – The calculated reduction of spontaneous decision-making or actions to enable the attainment of long-term goals can be a challenge, particularly for individuals who do not understand organisational or even team goals, and who rush to decisions that lack complete information and may ultimately undermine the work of subordinates and eventually will prevent successful outcomes.

Causal analysis – Being able to determine both personal and corporate paths to the benefit of both will develop individuals to gain a greater understanding of the whys and wherefores of a particular task. Such situational awareness assists an individual in being a more well-rounded and therefore more resilient person.

Empathy – Being cognizant of the impact that decisions (and actions) can have on individuals as well as the organisation without being dragged into personal issues is critical for every employee and leader at every level of the organisation. Empathy is very different from *sympathy* where emotions tend to cloud the ability of an individual, whether as a leader or team member, to overcome personal issues. Developing sound *emotional intelligence* must therefore be an essential goal of every aspiring leader.[8]

Self-efficacy – How to see beyond one's personal circumstances to influence the ultimate successful outcomes of an initiative should be based on empathy for fellow employees as well as an understanding of

---

[5] Daniel J. Levitin. *The Organized Mind: Thinking Straight in the Age of Information Overload.* Toronto: Allen Lane, 2024. p.7.

[6] Karen Reivich and Andrew Shatte. *The Resilience Factor: 7 Keys to Finding Your Inner Strength and Overcoming Life's Hurdles.* New York: Three Rivers Press, 2002. pp.295ff.

[7] Much of the information presented here comes from my Brookings Executive Education notes from 2012 to 2015, prepared largely by instructors from the Olin School of Business of Washington University in St Louis in preparation for the Master Science in Leadership granted by Olin from 2014 to 2020. Each one of the courses taken for the MSL required the writing of a research paper based on the course material and personal experiences in the candidate's professional and sometimes personal life. In preparing this article, I used many of my 18 essays and my thesis as background material.

[8] A good deal of literature exists on importance of emotional intelligence. A good summary may be found in Andrew Campbell, Jo Whitehead and Sydney Finkelstein. "Why Good Leaders Make Bad Decisions". In *On Emotional Intelligence*. HBR's 10 Must Reads Series. Boston, Mass.: Harvard Business Review Press, 2015.

how all personnel contribute to attaining an assigned goal.

Realistic optimism – Early successes may either lead to more successes or a sense of complacency, and it is important to know the difference. Without that understanding, an individual may feel left out, inadequate, or simply not part of a team, any of which will immediately undermine both personal and team resilience.

Reaching out – Realising that one can't do it alone or simply stand alone in any complex working environment and understanding highlights the importance of networking and partnering for success.[9]

In summary, what resilience means is that as individuals we can – and must – manage ourselves, well before we can consider ourselves as leaders.[10] Not having that ability will hinder us as we try to become resilient leaders, no matter how hard we try or how many courses we take. Well-inspired individual resilience, supported by the leadership chain, can be a very powerful tool in the effort to achieve results in any organisational setting. Similarly, resilience is directly related to *perseverance*, in that an individual may respond more effectively to any challenge by understanding *why* something is being done rather than simply carrying out a task.

Figure 1 depicts one interpretation of the relationship between resilience and perseverance, based on the fundamental aspect of the leadership mindset which seeks growth of oneself, one's team and the organisation as a whole. This concept is based on the idea that leadership and development are all about growth – expanding mindsets, achieving goals, and generally improving the lot of the team, the organisation and even a wider population.[11] It also relates to the ability of individuals and teams to take risks, by leaders giving team members permission to fail (as well as empowering them to be heard) This is accomplished by allowing them the opportunity to make informed decisions within a safe, experimental learning environment in which pertinent information is readily available and shared.

Figure 1[12]

Resilient Leadership Qualities

Similar qualities come to the fore in defining resilient leadership as may be seen for personal or individual resilience. These qualities include:

Integrity – Being honest and transparent in all our efforts, often in the face of considerable attacks on our individual and collective morality, will build leadership resilience. Equally true, being constantly challenged on personal principles will render a leader powerless to achieve the goals set by senior management, if that leader feels their principles are being undermined for unclear or even nefarious reasons.

Mentoring – Both a manner of succession planning but, more importantly, a method of introducing a sense of reality whilst not discouraging advancement and personal growth in subordinates and team members, is a key leadership responsibility in building resilience.

---

[9] Dr Jackson Nickerson. Building Networks and Partnerships. Brookings Executive Education, 2013.
[10] Daniel Goldman. *Resilience for the Rest of Us*. Harvard Business Review. 2011.
[11] Biljana Cvetanovski, Eric Hazan, Jesko Perrey, and Dennis Spillecke. "Are you a Growth Leader? The Seven Beliefs that Growth Leaders Share". McKinsey & Co report. September 2013.

[12] Duckworth, Angela. *Grit: The Power of Passion and Perseverance.* Toronto: HarperCollins, 2016. pp.192ff. I have adapted Duckworth's outline to demonstrate the importance of resilience to highlight the importance of risk and risk taking. I have used her wording in general but have expanded the concept to suggest the relationship between personal circumstances and those of the organisation as a whole. *Perseverance* is a quality often lacking in both leaders and organisations, unfortunately.

Realising the need to rely on trusted staff will increase a leader's resilience by producing a responsive and responsible team that can withstand challenges. Again, such mentoring can empower employees who feel they can take supported risks.

Values and Ethics – Having clearly defined values is essential for any leader, as is the requirement to realise that compromising one's values and principles is of no help to anyone. Without doubt, any sense of resiliency must be built on a foundation of strong values and ethics which are both clearly defined and espoused each and every day.[13]

Connection – Helping teams and team members remain connected to the goals which have been set and thereby achieve the results that are expected of the team is one way of ensuring team resilience. Team successes will always create a sense of which lends to recognition of accomplishments and achievements by individuals, regardless of the personal feelings of the leader.

Results – While obtaining results is always critical, *how* those results are achieved is equally important and must be taken into consideration, based on the abilities and talents of the team being tasked as well as the constraints and limitations that are imposed by senior management or leadership.[14] One key factor in looking at results is that the resilient leader will know when to set aside personal concerns to deal with more important challenges that affect more than just him/herself. One obvious outcome of a situation where the leader fails to find the balance between his/her personal requirements and the needs and goals of the team is the development of an immediate sense of disillusionment on the part of the team who feel unsupported, and possibly to blame for any unfortunate outcomes. This situation must be avoided at all costs.

Organisational Resilience

Organisations are built up of individuals and teams of individuals, and therefore every member of an organisation must be able to contribute to its growth, development and sustainability and to see themselves in the results achieved. In order to build a resilient organisation, whether one is looking at a whole corporation or an individual team, several steps are required which must be open and transparent to all members of the organisation.

Firstly, the senior leadership of the organisation must define the values and ethics at the corporate and individual levels, to enable the support their subordinates. They must reflect these values and ethics in all their dealings, both internally to the organisation and externally in relationships with partners. Research has demonstrated that the five most important values for corporations and individuals are: Responsibility, Truth, Fairness, Compassion and Self-respect.[15] While the exact words may differ from one organisation to another, the sense of all the values is reflected in the creation of healthy and resilient organisations. If corporate values are not clearly communicated to staffs, and upheld in all actions, the organisation will not support the goals and tasks assigned to them.

Secondly, a resilient organisation is one where the communications are open and transparent to the greatest extent possible. This stance includes the communicating of goals, timelines and other aspects leading to successful outcomes of taskings, in order to ensure that staffs are aware not only of *what* they are

---

[13] Harry M. Jansen Kraemer, jr. *From Values to Action: The Four Principles of Values-Based Leadership.* San Francisco: Jossey-Bass, 2011. pp. 153-54. See also Susan Liautaud with Lisa Sweetingham. *The Power of Ethics: How to Make Good Choices in a Complicated World.* New York: Simon & Schuster, 2021. pp. 203-5. Resilience in an ethical sense, including the context of ethical decision-making, is particularly difficult – and important – in the recovery from a failure of leadership, management or any corporate crisis.

[14] One method of determining the state of any team is to conduct a 'team audit'. The best guideline I have used in my career is the one developed by Dr Frances Johnston at the Teleos Institute which I used to great benefit in trying to fix a damaged and vulnerable organisation. For more information, see https://teleosleaders.com.

[15] See, for example, Rushworth M. Kidder. *Moral Courage.* New York: HarperCollins, 2005. pp.46-55.

doing but also *why*. Figure 2 depicts one example of how values contribute to the overall organisational goals by clearly defining the relationships between leaders, team members and even clients or stakeholders, and by showing the interdependencies in communications and transparency, based on an understanding of the organisation's needs.[16]

Such communications also means that employees must feel able to push back, to challenge unrealistic expectations or goals, and to know that they will not be punished for so doing. An organisation that supports strong communications including open and frank discussions will prove to be more resilient in the long run than one that is unnecessarily authoritarian in nature. 'Speaking truth to power' is not something that every organisation encourages; in many respects its acceptance simply reflects the level of tolerance of risk in the organisation.[17]

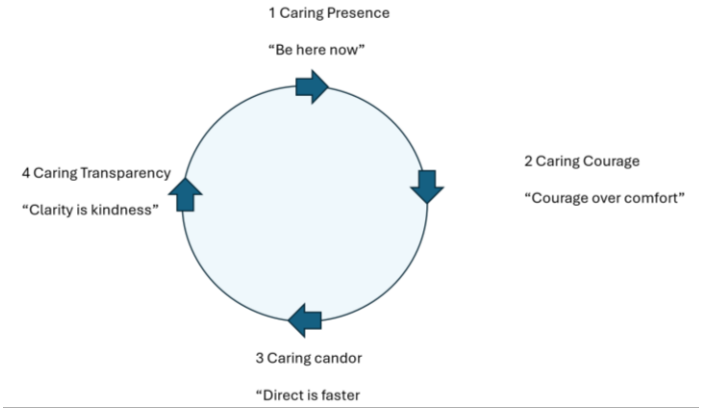

Figure 2 Leadership Communications Effects

Thirdly, a resilient organisation, which is of course made of individuals and teams, must be responsive to the needs of the employees. These needs must be recognised at the highest levels, and that recognition must be communicated to staffs in clear and understood ways. Even more importantly, leaders must *demonstrate* that they have the best interests of their employees at heart, and not merely pay lip service to a list of values, ethics and resource requirements.

Building the Resilient Individual, Team and Organisation

The primary question is whether resilience can be learned or is it something with which individuals are born. Neuroscientists have recently studied the existence of a 'resilience gene', which enables people with the gene to weather traumatic personal or professional events better than those without it.[18] While the evidence is limited at the present time, there are certainly indications that resilience can equate to the ability to respond in times of trouble. One aspect of this research has focused on the relationship between 'trauma' and 'resilience', searching in part for linkages between traumatic events that happened earlier in life and how different individuals respond to a variety of stresses. Clearly an individual who has a built-in sense of resilience is less likely to suffer long-term from the effects of a traumatic event, and is usually more likely to recover more quickly than someone who lacks the basic resiliency.[19]

That said, it is indeed possible for most individuals, leaders and organisations to become more resilient and therefore able to grow and prosper, but, as we have seen, to do so requires deliberate attention being

[16] Adapted from Hougaard and Carter, *Compassionate Leadership*, p.124.

[17] Risk taking is an essential attribute of leadership, but only when it is well considered and applied in appropriate circumstances. That said, many organisations are risk adverse for political, policy or economic reasons, often to the detriment of their staffs. A proper balance must therefore be found to suit all occasions. See Ron S. Dembo. *Risk Thinking…in an uncertain world*. Bloomington, IN: Archway publications. 2021.

[18] Julian Barling. *The Science of Leadership: Lessons from Research for Organization Leaders.* Oxford: Oxford University Press, 2014. p.142. See also Ryan M, Ryznar R. The Molecular Basis of Resilience: A Narrative Review. Front Psychiatry. May 6, 2022; 13:856998.

[19] The relationship of trauma to PTSD is also key. See, for example, the research being conducted by the Crisis Trauma and Research Institute at CTRI Training | Crisis And Trauma Resource Institute (ctrinstitute.com)

applied.[20] In some cases, resilience simply develops with anyone, at any level in an organisation, by focusing on positive aspects of a situation rather than on the negative ones. This in turn creates a more focussed organisation that can withstand challenges.[21] It also allows for more personal growth within an organisation.

Similarly, learning the skills of reflection can also increase resilience, by reviewing both successes and challenges and putting them in context. It is a truism of leadership and organisational studies that one can learn many more lessons from adversities than from following simple paths to success. Organisations which offer a safe space for experimentation are far more likely to achieve advances than those that punish failures.[22] Allowing employees to try to find solutions to what might seem to be intractable situations will not only encourage teamwork, will empower them within the organisation. By extension, empowered employees are more likely to be resilient to threats of one sort or another than those who are afraid to speak out.

For leaders of teams and organisations, being resilient means knowing when to put one's needs before those of the project. In the current employment context, employers must be mindful of the physical and technological resources including adequate workspaces that the employees need, but, more importantly, they need to be aware and therefore realistic about the mental health of staffs. Current generational changes have brought this aspect of leadership more to the fore than has previously been the case. The first step is hence to ensure that organisations have programmes in place to develop resilience: appropriate time off for health and vacation; encouraging employees to participate in physical activities; and encourage employees to work together and celebrate together, when appropriate. In post-pandemic times, when staffs are used to more remote work or work from home rather than spending time in the office, leaders have to be aware of the 'zoomed out' effects of work on-line, as well as the challenges of managing and leading people who are not in the office.[23]

Secondly, organisations can support leaders at all levels by encouraging them to look after themselves as well their teams. All too often, leaders face burnout which reduces their effectiveness within the organisation. In that case, organisations might lose good leaders, harming overall corporate success and growth. Leaders have the tendency, particularly at lower levels, to take on too much in order to in the eyes of senior management and leadership. This can be the case at the onset of projects, when leaders use the 'iceberg' model of systems thinking: attempting to do too much in the initial stages of a project raises expectations and can contribute to creating misunderstandings and misinterpretations, whilst diminishing their personal (physical) resilience.[24]

This aspect of resilience, which focuses on the individual, is critical, as their resilience ultimately affects the organisation as a whole, over and beyond the individual. Employees and leaders need to know that their organisation supports them, both within the team environment and in a much broader sense. If they feel they are being ignored, or even undermined by the chain of command, the effects on resilience will be immediate

---

[20] Of course, it is also true that some individuals will never be resilient to any type of change, difficulty, challenges etc. These people must nevertheless by supported to a greater or lesser degree, but a leader may at some point have to make decisions concerning that employee's value or suitability for a particular role, and may have to take action accordingly.

[21] Kathleen M Sutcliffe, and Timothy J. Vogus. "Organizing for Resilience". In Kim S. Cameron, Jane E. Dutton and Robert E. Quinn, eds. *Positive Organizational Scholarship: Foundations of a New Discipline.* San Fransisco: Berrett-Koehler Publishers, 2003. pp. 95-97.

[22] Dr Marcus Baer. Inspiring Creativity in Organizations. Brookings Executive Education. 2024.

[23] Frances Johnston, *Zoomed Out & Exhausted: Taking a Closer Look at our New Reality*. Teleos Institute, March 29, 2021. Zoomed Out & Exhausted: Taking a Closer Look at our New Reality - Teleos Leadership Institute

[24] The concept of 'Iceberg' thinking and the concomitant systems approach is well developed, and usually applies to endeavours that require in-depth research in the approach to complex situations, but initially at least the emphasis is on only what is visible and therefore of interest to senior leadership and management who want quick solutions.

and harsh. As part of the resilience journey, employees and leaders need to understand that corporate leadership display their sense of integrity, their leadership principles, and the values for which they stand, even in the face what might ultimately be unsolvable challenges. Leaders also need to understand the limitations of their team so as to manage expectations. Equally important, employees must be able maintain faith in the values and principles of their leadership chain, whilst knowing that their abilities are respected and encouraged. For without either or both of these beliefs, individuals will not be able to maintain a personal sense of resiliency and balance and, by extension, will not be able to lead teams through challenging circumstances. Similarly, keeping things in perspective, either with an increased sense of detachment or even simply with a good sense of humour, will contribute to a more resilient leadership style.[25]

Being more aware of individuals' needs will somewhat temper a leader's drive for change and will in some cases actually slowed down its pace. It also reinforces the need to celebrate even small successes, and the need to share a greater part of leadership responsibilities without abrogating any leadership accountabilities. Empowering staff is a key milestone for the team – and for the leader – as employees receive increased responsibility and personal accountability, whilst ensuring that the leader retains overall organisational accountability for the successful delivery of goods and services. Recognising individual achievements is an essential factor in sustaining and empowering teams, so that team members know that what the leader does is not 'about me' but that *they* are the important elements in building success.

One way in which resilient leaders can develop resilient employees is by developing what Dr Fiona Hill as described as the 'infrastructure of opportunities'.[26] If employees see that their leaders want to encourage them to grow, they will respond in kind. It is therefore important for the leadership at all levels to demonstrate that opportunities for growth exist, whether through education or training, on-job-training, special assignments, etc.[27] Such encouragement will contribute to developing more resilient and responsive employees.

Finally, all leaders must find time for reflection on the effectiveness as well as the appropriateness of their leadership style. By taking any available opportunity for reflection on both the positive and negative aspects of the position and the tasks at hand, the leader can accept any errors made personally or by the team, and therefore be able both to move beyond them and avoid them in the future, and to take advantage of the positives that have resulted. In so doing, a leader can adapt his or her leadership style, including leading by example through balancing hard work and needs of the team. Developing an ability to step back and re-assess is a key factor in the continuing development of any leadership style. Similarly, an understanding of the need to accept the limitations of an organisation will also be of help.

Taking the time for reflection will result in the creation of resilient employees, leaders and ultimately organisations. One clear realisation will show that, while a leader may contribute to the fulfilment of overall organisational responsibilities, it is not up to them to solve all the problems on their own. The sense of having to be 'all things to all people' cannot contribute to the resiliency of a leader; it may in fact have the opposite effect.

---

[25] Dr Frances Johnston. Creating High Performance Teams. Brookings Executive Education, 2015.

[26] Hill, Fiona. *There is Nothing For You Here: Finding Opportunity in the Twenty-First Century.* Boston: Mariner Books, 2021. pp65, 82 and elsewhere. Hill left her impoverished roots in the Northeast of England and through hard work and taking advantage of opportunities presented to her - most of which were unexpected or came from unexpected sources - to become a highly respected Russian expert. She served as one of the first women at the Brookings Institution, as well as as the leading Russia expert in the Trump White House's National Security Council. She is currently a senior advisor the newly elected British Prime Minister, Sir Keir Starmer.

[27] Dr Lee Konczak. Leaders Growing Leaders. Brookings Executive Education. 2013.

These lessons are exactly what leaders must transmit to their ‘mentees’ as who together face challenging times in our rapidly changing and financially constrained workplaces. Leading by example through practicing the steps of resiliency will be the most valuable skill a leader can transmit to the next generation.

About the Author

Valerie Keyes is the President and CEO of GTM Leadership Matters, an Ottawa-based consulting firm specialising in leadership training. She is also a Senior Associate in the Samual Group of Companies. Valerie was a member of the Canadian Armed Forces, being the first woman to receive a degree from the Royal Military College of Canada. She served as a policy, intelligence and security analyst and Director in the Public Service, in National Defence, the Privy Council Office, Natural Resources Canada and Public Works Canada. She also served as a senior advisor to the British Army on matters of ethos and leadership. Valerie is the only Canadian to have received the Master of Science in Leadership from the Olin School of Business at Washington University in St Louis.

Recommended Critical Infrastructure Security and Resilience Readings

Felix Kwamena, Ph.D.*
Email: felix.kwamena@carleton.ca

Robert Osei-Kyei, Laura Melo Almeida, Godslove Ampratwum, *Tam Systematic review of critical infrastructure resilience indicators* Systematic review of critical infrastructure resilience indicators | Emerald Insight

Robert Osei-Kyei, Vivian Tam, Mingxue Ma, Fidelis Mashiri, Critical *review of the threats affecting the building of Critical infrastructure resilience* International Journal of Disaster Risk Reduction, Volume 60, 15 June 2021, 102316

Yuning Jiang, Manfred A. Jeusfeld, Michael Mosaad, Nay Oo, Enterprise architecture modeling for cybersecurity analysis in critical infrastructures — A systematic literature review, International Journal of Critical Infrastructure Protection, Vol 46, September 2024, Enterprise architecture modeling for cybersecurity analysis in critical infrastructures — A systematic literature review - ScienceDirect

Dwij Mehta, Aditya Mehta; Pratik Narang; Vinay Chamola; Sherali Zeadally, Deep Learning Enhanced UAV Imagery for Critical Infrastructure Protection | IEEE Journals & Magazine | IEEE Xplore

Nii Attoh-Okine, Special Section on Digital Twins: A New Frontier in Critical Infrastructure Protection and Resilience The American Society of Mechanical Engineers Vol 10, Issue 1 February 1, 2024, Special Section on Digital Twins: A New Frontier in Critical Infrastructure Protection and Resilience | ASME J. Risk Uncertainty Part B | ASME Digital Collection

Natalie Coleman, Xiangpeng Li, Tina Comes and Ali Mostafavi, **Weaving equity into infrastructure resilience research: a decadal review and future directions , Natural Hazards Journal Vol 1 Issue 23 September 2024, Weaving equity into infrastructure resilience research: a decadal review and future directions | npj Natural Hazards**

Dr. Antonio Carlo a, Dr. Kim Obergfaell Cyber attacks on critical infrastructures and satellite communications International Journal of Critical Infrastructure Protection Volume 46, September 2024, 100701

Michalis Papamichael a, Christos Dimopoulos b, Georgios Boustras b, Marios Vryonides Performing risk assessment for critical infrastructure protection: A study of human decision-making and practitioners' transnationalism considerations International Journal of Critical Infrastructure Protection Volume 45, July 2024, 100682

João Henriques; Filipe Caldeira, ; Tiago Cruz; Paulo Simões **A Survey on Forensics and Compliance Auditing for Critical Infrastructure Protection IEEE Xplore Vol 12, 2024**

Norrman, A. and Eriksson Ahre, E. (2024), "Contextualizing supply chain risk governance in critical infrastructure sectors: insights from the Swedish food system", *The International Journal of Logistics Management*, Vol. 35 No. 7, pp. 33-59. https://doi.org/10.1108/IJLM-10-2023-0444

Julia Grimm, Ann Langley, Juliane Reinecke Process Research Methods for Studying Supply Chains and Their Management, Journal of Supply Chain Management: Volume 60, Issue 4, October 2024, Pages 1-106

Aleksander Cwalina, concerns grow over possible Russian sabotage of undersea cables, / ***Rising Military Activity Around Undersea Cables*** **Atlantic Council, September 12, 2024, Concerns grow over possible Russian sabotage of undersea cables - Atlantic Council**

Paganini Russia-linked GRU Unit 29155 targeted critical infrastructure globally Indictments Unveil Unit 29155 and Scale of Russian "Hybrid Operations" Security Affairs September 2024.

Catherine Morehous Tensions at home and abroad pose growing threat to US grid *Physical Security Incidents Targeting Electrical Substations in US Rising E&E News, August 2924 Tensions at home and abroad pose growing threat to US grid - E&E News by POLITICO*

Sean Monaghan, Michael Darrah, Eskil Jakobsen, and **Otto Svendsen Red Sea Cable Damage Reveals Soft Underbelly of Global Economy Centre for Strategic & International (CSIS) Studies March 2024.**

Red Sea Cable Damage Reveals Soft Underbelly of Global Economy

Cybersecurity Advisory February 07, 2024 PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure America's Cyber Defence Agency PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure | CISA

Master Plant Development Agreement Amazon, Google follow Microsoft with commitments to support deployment of nuclear energy: Recognizing the challenges with securing the power needed to support their expanding data storage and computing needs and meet their climate commitments, Google and Amazon followed Microsoft in striking agreements with utilities and nuclear energy companies to ensure access to zero-emission electricity options in the future:

New nuclear clean energy agreement with Kairos Power Google signs advanced nuclear clean energy agreement with Kairos Power

Amazon and Energy Northwest announce plans to develop advanced nuclear technology in Washington Amazon and Energy Northwest announce plans to develop advanced nuclear technology in Washington

Amazon Invests in X-energy to Support Advanced Small Modular Nuclear Reactors and Expand Carbon-Free Power Amazon Invests in X-energy to Support Advanced Small Modular Nuclear Reactors and Expand Carbon-Free Power — X-energy

U S DOE announces new $1.05B loan for EV chargers , DOE's Loan Programs Office announced a conditional commitment of up to $1.05B to EVgo to expend its public charging infrastructure. This is expected to support the deployment of approximately 7,500 fast chargers in 1,100 charging stations across the U.S. over the next five years, including in California, Illinois, Michigan, New Jersey and New York, with a focus on disadvantaged communities.

LPO Announces Conditional Commitment to EVgo to Deploy Nationwide EV Fast Charging Network | Department of Energy

LPO Announces Conditional Commitment to EVgo to Deploy Nationwide EV Fast Charging Network | Department of Energy

The United States of America and Peru Sign Memorandum of Understanding to Strengthen Cooperation on Critical Minerals The United States of America and Peru Sign Memorandum of Understanding to Strengthen Cooperation on Critical Minerals - United States Department of State

The Conference Board of Canada Skills and Productivity: Which Skills Shortages Are Impacting Canadian Productivity?—August 2024 Skills and Productivity: Which Skills Shortages Are Impacting Canadian Productivity?—August 2024 - The Conference Board of Canada

Adam Vanzella Yang, Daniel Akira Stadnicki, Who Is Using Generative AI in Higher Education? The Conference

Dan Carpenter, evolving landscape of artificial intelligence. Technology The Conference Board of May 28, 2024

++

2024- 2025

EVENT	DATE / LINK
Training Courses **Schedules and Training Partner Dates Posted**	https://carleton.ca/irrg/training/
2024 Knowledge – Café Workshop ***Space is limited and registration is first come first served. Hope to see you there!*** **Thursday, November 21,2014, 8:30 – 4:30** **Metcalfe Hotel, Edward Room, 123 Metcalfe St. Ottawa, ON K1P 5L9** **Program (pdf): 2024 K-C WORKSHOP PRELIMINARY PROGRAM**	**Register now for the 2024 Knowledge Cafe and Workshop at www.savoiesecurityassociates.ca.** https://carleton.ca/irrg/?p=2452
IRRG Dean's Lecture The Dean's Annual Lecture Series – Infrastructure Security and Resilience: Economic Security, Resilience. **In Abeyance**	https://carleton.ca/irrg/cu-events/2020-deans-lecture/

Check out IRRG's Website for:

Upcoming events

https://carleton.ca/irrg/events/

Professional Training / Development Courses

https://carleton.ca/irrg/training

Latest Issue of Online Journal
Infrastructure Resilience Risk Reporter ***(IR^3)***

https://carleton.ca/irrg/journal/