CIGRE-397 **2021 CIGRE Canada Conference & Expo**
Toronto, Ontario, October 25-28, 2021

Cybersecurity risk reduction leveraging cyber range solutions

D. Boucher, G. Farthing
vadimUS, Canada

P. Berthier
RHEA Group, Canada

G. Hillier
CIMA+, Canada

SUMMARY

Cybersecurity is becoming increasingly challenging in the energy sector. It is well known that the increased network connectivity due to convergence of information technology (IT) and operations technology (OT) systems in energy networks, along with other critical infrastructure sectors, increases the attack surface available to cyber adversaries.

Distributed access to control systems, applications services, and the reality of complex software results in increased cyber risks to energy networks. Several nation states have established an offensive cybersecurity doctrine including the identified need to interfere with and damage critical infrastructures, including energy networks.

The result of the increased and evolving cyber threat is a corresponding increased attention applied to cyber security risks in all stages of development and operation across the industry. The importance and urgency of implementing proper cybersecurity measures is further warranted by realistic projections of continued pressures stemming from an evolving physical and cyber threat landscape and increasing industry regulations.

Among the promising approaches to improve cybersecurity preparation and risk reduction in critical infrastructures is the use of Cyber Range solutions. A Cyber Range provides a virtual environment to train and equip cybersecurity professionals and system operators (ex. train personnel on responding to incidents, both electrical load and cyber incidents); perform cybersecurity tests and evaluations of both legacy systems and new architectures in a simulated operational environment; and perform cybersecurity related research and development of automated control systems and prototype technologies intended to improve security of energy networks.

This paper describes the benefits that can be achieved in cybersecurity risk through use of Cyber Ranges; discusses various case studies and scenarios relevant to the energy sector; and highlights the opportunities for personnel training and capability building that can be achieved.

KEYWORDS

Cybersecurity, Cyber Range, SCADA, NERC-CIP, Training, Test, Design, Digital Twin, Hardware-in-the-Loop, Co-Simulation.

p.berthier@rheagroup.com
greg.hillier@cima.ca
gfarthing@vadimus.biz
dboucher@vadimus.biz

1. URGENCY TO IMMUNIZE THE ENERGY SECTOR AGAINST CYBER ATTACKS

It is well-known that the power sector has become a common target to cyber-threats and that those threats are evolving, now reaching into control systems, supply chains and further intrusion points so exposing utilities to greater efforts to manage bigger risks.

Coupled with more individuals working remotely due to the pandemic, utilities are facing another perfect storm with cyberattacks and other data-related incidents. The pandemic accelerated the digitization of almost every aspect of our lives, requiring the rapid introduction of new technologies at the office and at home where utility employees expect to continue working.

Without appropriate cybersecurity practices, utilities cannot adequately prepare for cyber-attacks and, if exposed, may face significant financial loss, reputational harm, grid disruption and potential lengthy regulatory investigations and litigation. Many countries across the globe have officially classified electrical grid infrastructure as critical to a functioning society. In Canada, a recent exhaustive study [1] has revealed four broad categories of trends:

1. Cybersecurity incidents,
2. Privacy breaches,
3. Cybersecurity-related disclosures,
4. Cybersecurity litigation trends.

Electrical utilities report a continuous barrage of attempted intrusions, and though most fail, activity is accelerating up to hundreds and thousands of times a day. Not only the attacks are rising but the number of threat actors is increasing and their capabilities expanding.

Attackers are increasingly targeting control systems, sometimes laying the groundwork to do physical damage to the grid. Previously, attackers primarily targeted utilities' Information Technology (IT) systems to steal data or launch ransomware against money. It is now becoming more insidious with attempts to control physical assets across the network such as power plants, substations, transformers, supervisory control and data acquisition (SCADA) systems and even critical circuit breakers through command-and-control relays, the Operational Technology (OT) elements.

Cyber risks exist across utility companies meaning People, Processes and Technology (PPT) must all become more secure, more vigilant, and more resilient areas. The North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC-CIP) have put the power sector at the forefront in establishing regulations to reduce cyber risks. However, these standards only apply to high-and-medium Bulk Electric Systems (BES), and not their external risks across the expanded supply

This paper proposes a cyber range solution to focus on three highly important and permanent activities: testing, designing, and training. chain such with new factors pertaining to remote personnel, distributed energy and more interacting consumers.

2. COMPREHENSIVE EMULATION VS SIMULATION MODELLING

A modern utility's infrastructure is a complex system that integrates physical OT components, IT devices, software, and networking equipment. Moreover, remote working, distributed access to control systems, applications services, and the reality of complex software bring an additional layer of complexity.

Due to this high complexity, the development of such infrastructures requires knowledge and expertise from different teams and must be distributed.

Innovative and truly optimal multi-disciplinary solutions can only be achieved through a holistic development process where the partial solutions developed independently are integrated sooner and more frequently.[2]

A common approach in the SCADA community to overcome this challenge is the use of Co-Simulation.

Co-Simulation consists of the theory and techniques to enable global simulation of a coupled system via the composition of simulators.[2]

With a Co-Simulation approach, each team builds its own black box component to be part of the global system. There is little interaction between the teams up to the integration phase, and teams are usually unaware and lacks understanding of other teams' development content. This is true within internal IT and OT teams and with integrators and suppliers. The approach serves to design, test, and perform security and compliance tests without revealing complex details or intellectual property relative to black box components.

The first obvious drawback from this approach is the complexity for the integration of the different components. A backend-loaded integration effort at the end of project is likely to cause issues, design changes and cost overruns.

This is accentuated by the recent acceleration in the evolution of the different technologies.

A specific challenge here is the rapidity of the development cycle of ICT and power electronic devices, because the behavior of the individual subsystems and their interaction with each other change quickly over time.[3]

An integration environment which allows for fast integration throughout the project and permits parallel testing of different environment configurations (either with components from different vendors or different versions) would be more suitable.

The second drawback for this approach occurs at the subsystems' level when subsystems where simulators are unsuitable for specific use-cases due to unmet requirements for high-fidelity reproduction of the internal behaviour of the system. This is the case for cybersecurity testing of IT and networking components, where attackers target the external behaviour of a black box and exploit the internal implementation of the component.

***Simulation** = The act of modeling, through a software, the general behavior of a system (output) starting from a conceptual model.*

One frequent example is the implementation of cryptography algorithms, where small errors in the implementation can diminish the encryption's strength. When developing software, minor design errors combined with improper sanitization of user inputs can lead to buffer overflow and vulnerabilities in the system.

***Emulation** = The act of replicating or virtualizing, in a different system, exactly how the original system works internally*

From a black box perspective, a predefined set of inputs into the black box generates the proper set of outputs, as defined in the requirements. However, the actual implementation within the black box may cause issues at the integration phase.

3. THE SOLUTION: AN ADVANCED CYBER RANGE PLATFORM

The virtualization technology within an advanced cyber range platform resolves the two important drawbacks with:

- easy integration of sub-components throughout the project development
- emulation to reproduce with fidelity the internal implementation of the components.

The integration of Cyber-Physical Energy Systems (CPES) via the technique of virtualization has the potential to notably advance power system automation. Future power systems - especially Smart Grids - will increasingly rely on software and therefore extend the interwoven dependencies between the power system and its Information and Communication Technology (ICT) infrastructure.[4]

An advanced cyber range platform supporting secure systems development and delivery should include:

1. A scalable and flexible energy network emulation environment.

   To support test and evaluation of legacy and candidate technologies, systems and solutions, the cyber range must consist of a system-of-systems solution comprised of a range of emulation technologies including:

   - control systems,
   - controlled devices,
   - SCADA servers and historians and
   - interconnection networks.

2. An adaptable test harness with standardized interfaces:

   To conduct testing of technologies within the emulation environment, it is essential that discrete components within the end-to-end service can be independently replaced by technologies under test. This is particularly true for legacy systems that may not be easily adapted to a virtual simulation environment but must be included as “hardware-in-the-loop”.

3. A cyber simulation capability:

   Cybersecurity test and evaluation of assets involved in energy networks require a range of security testing capabilities. This includes application testing tools, as well as technical vulnerability assessment and penetration testing tools.

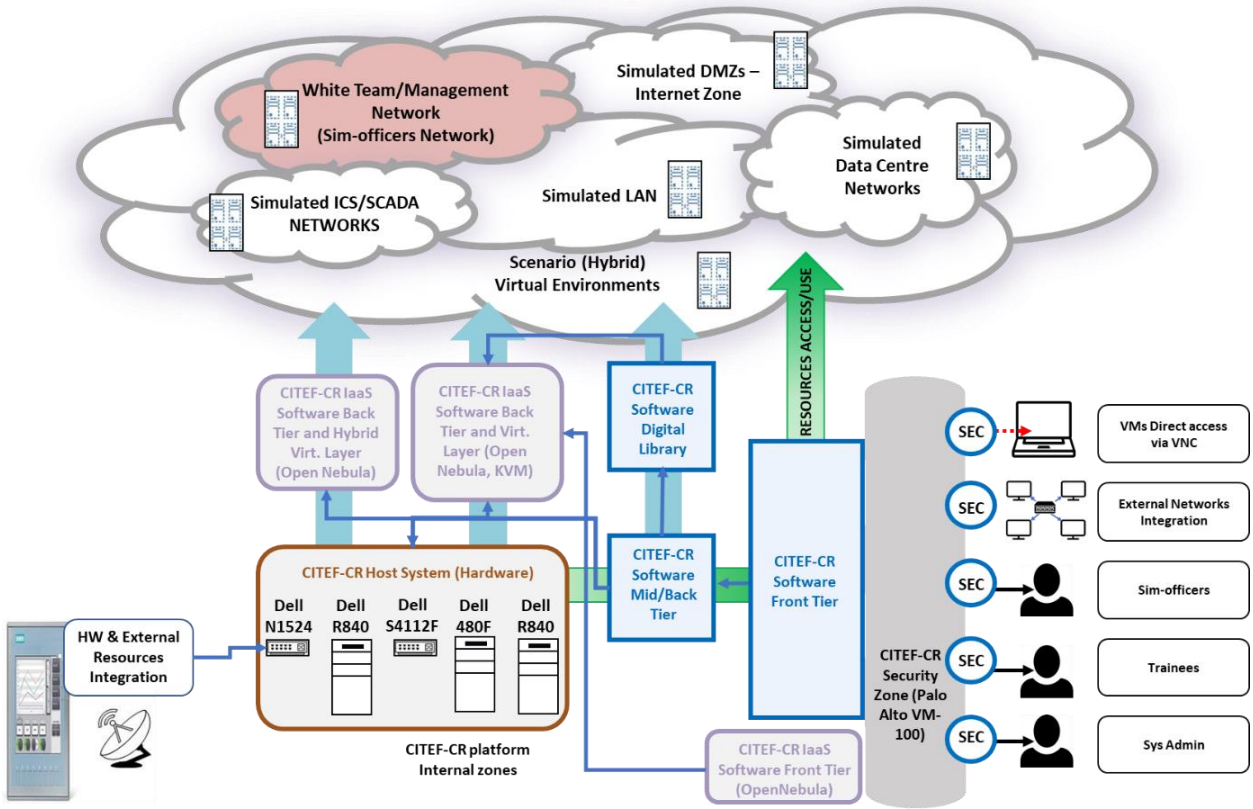

Figure 1: Example of an advanced cyber range platform

4. USE CASES DEMONSTRATING THE CYBER RANGE CAPABILITY

We have seen that the blurred lines between IT and OT open a whole new attack vector for utilities to worry about.

The difficulty in running a vulnerability management and cyber security program is increasing daily with incidents occurring from both outside and inside. Whether purposeful or accidental, most incidents can be prevented with the right tools and training. To overcome many obstacles when hardening an environment, the IT world created labs and simulated environments to perform design, testing and training.

One example applies to penetration testing on a new device. Testing may have to hold back on the more intrusive attacks if the device is already in production. To record its live reaction to such an event, both internally and towards its neighbors, the test must be performed in a real environment.

An emulated cyber range provides the most realistic environment while keeping your productions network safe.

Since many utilities have turned to Frameworks, Certifications and Standards like IEC 61850, NIST-800 and NER-CIP to enhance their cyber security profile or become compliant with regional industry requirements, the following outlines how a cyber range can enrich the cybersecurity program using NERC-CIP as an example:

- NERC CIP 004-6: “Cyber Security – Personnel & Training” mandates a collection of training requirements on applicable entities.

  Application: Although the training does not specify that hands-on training is required, it is well known that hands-on training provided by a cyber range is more effective in regard to participant retention of knowledge.

- NERC CIP 005-5: "Cyber Security – Electronic Security Perimeters" mandates a collection of technical requirements on applicable entities intended to establish protective controls at the perimeter of the entity.

  Application: Use of the cyber range to emulate and test the perimeter controls can be used as evidence related to this requirement. Strict speaking, such evidence exceeds the standard requirements as a more effective means to evaluate and demonstrate the efficiency of these controls.

- NERC CIP 007-6: "Cyber Security – Systems Security Management", Requirement R2 "Security Patch Management" mandates a set of requirements related to security patch management for applicable entities.

  Application: In particular, part 2.2 specifies that at least once every 35 calendar days, security patches are evaluated for applicability. As part of a good patch evaluation process, patches should first be tested in a non-production environment to determine if the patch will have a negative effect on operations. A cyber range with a high-fidelity emulation of the OT systems provides a safe and effective means to evaluate patches and assess if any negative impacts could affect operations.

- NERC CIP 008-5: "Cyber Security – Incident Reporting and Response Planning" mandates a collection of process and technical requirements on applicable entities related to management of response to cyber security incidents. This includes, for example a set of requirements related to incident response planning (R1), implementation and test (R2).

  Application: A cyber range with high-fidelity emulation of the operational environment can support the development and test of the incident response plans. An added advantage stems from the emulated environment's natural capability to provide a safe environment to train operations staff and maintain skills in the execution of incident response plans.

- NERC CIP 009-6: "Cyber Security – Recovery Plans for BES Cyber Systems" mandates a collection of process and technical requirements on applicable entities (BES – Bulk Electrical System) related to managed of system backup and recovery actions.

  Application: In some cases, the requirements state that the plans be tested "in an environment representative of the production environment" (R2.3). In this context, a cyber range provides an ideal representative of the production environment to meet the requirement. Whether or not a representative environment is specified in other requirements, as per NERC CIP 008-5, a cyber range with a high-fidelity emulation of the operational environment can support the development and test of the recovery plans. Here again, the cyber range delivers the additional advantage of providing a safe environment for training and maintain skills within operations' staff,

- NERC CIP 010-2: "Cyber Security – Configuration Change Management and Vulnerability Assessments" mandates a collection of process and technical requirements related to configuration changes and vulnerability assessments.

  Application: For configuration changes, requirements include analysis of potential impacts. R1.5 specifies that prior to implementing any changes in the production environment, a change shall be tested in a test environment where technically feasible. A cyber range naturally provides that safe environment in which configuration changes can be tested. Similarly, the cyber range provides a safe environment to perform vulnerability assessments as outlined in R3.5 wherein active vulnerability assessments should be performed in a test environment where technically feasible.

5. CONCLUSION

The recommendations mentioned in this paper are good first steps to implementing comprehensive, risk-based cybersecurity practices.

They provide a detailed look at how an organization's resources can be structured to address grid security in a manner that balances protection with the need to provide affordable energy to consumers.

Prioritization and proper planning, including design, testing, and training, are vital to ensuring further collaboration, communication, and understanding to maintain a resilient and reliable power grid within an electrical utility.

They will help navigate through the complex relationship between their IT and OT environments and support the digital transformation (design and expansion of the grid and generation mix). They will improve:

- team coordination and experience,
- teamwork and results,
- introduction, robustness, and integration of new designs/innovations, and
- execution of incident response plans.

The ability to prevent, respond to, document, recover and learn from cybersecurity advance testing, event scenarios, and operational disruptions will safeguard essential business services against severe, and probable threats.

Outside threat actors and forces will not stop trying to infiltrate and breach utility infrastructures and control devices.

A proper emulation environment within a cyber range including tools, detection, isolation, and documented remediation plans, ensure the vitally important successful and uninterrupted delivery of energy required to sustain societal stability.

Power delivery remains stable, and the lights stay on.

6. BIBLIOGRAPHY

[1] Blakes, ‘Canadian Cybersecurity Trends Study’, 2021. https://communications.blakes.com/29/122/_uploads/Blakes_Cybersecurity_Trends_Study_2021_EN.pdf?intIaContactId=3UYlIjjoc5zWGbEXJr550w%3d%3d&intExternalSystemId=1 (accessed Jul. 16, 2021).

[2] C. Gomes, C. Thule, D. Broman, P. G. Larsen, and H. Vangheluwe, ‘Co-simulation: State of the art’, *arXiv:1702.00686 [cs]*, Feb. 2017, Accessed: Jul. 14, 2021. [Online]. Available: http://arxiv.org/abs/1702.00686

[3] P. Palensky, A. van der Meer, C. Lopez, A. Joseph, and K. Pan, ‘Applied Cosimulation of Intelligent Power Systems: Implementing Hybrid Simulators for Complex Power Systems’, *IEEE Industrial Electronics Magazine*, vol. 11, no. 2, pp. 6–21, Jun. 2017, doi: 10.1109/MIE.2017.2671198.

[4] B. Jablkowski, O. Spinczyk, M. Kuech, and C. Rehtanz, ‘A Hardware-in-the-Loop co-simulation architecture for power system applications in virtual execution environments’, in *2014 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, Apr. 2014, pp. 1–6. doi: 10.1109/MSCPES.2014.6842403.