Government of Canada
Gouvernement du Canada

Overview and Areas of Strategic Engagement

NATIONAL ENERGY INFRASTRUCTURE TEST CENTRE

Canada

Government of Canada Gouvernement du Canada

Overview and Areas of Strategic Engagement

NATIONAL ENERGY INFRASTRUCTURE TEST CENTRE

Canada

Cat. No. M164-11/2016E-PDF (Online)
ISBN 978-0-660-06350-8

Aussi disponible en français sous le titre : Vue d'ensemble et domaines d'engagement stratégique

Content

Part 1 NEITC overview

Part 2 NEITC strategic engagement areas

Part 1 NEITC overview

NEITC ADVANTAGE

INTELLIGENCE-DRIVEN, HANDS-ON, INDEPENDENT EXPERTISE AND COLLABORATION FROM BEGINNING TO END

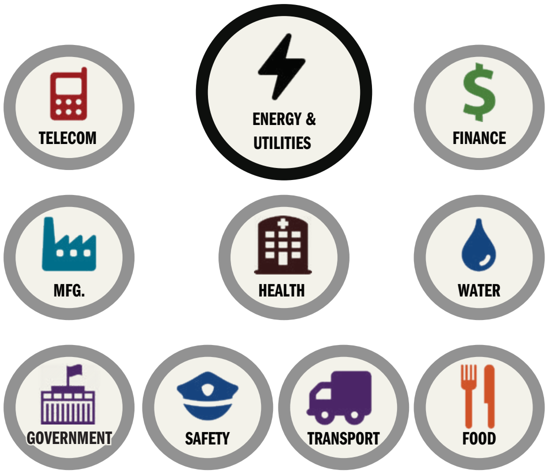
1. Introduction

Canada's energy infrastructure is the backbone of our modern society. It is responsible for delivering the vital fuel and power that keeps the lights on, our houses warm, and our vehicles running. The federal government plays a key role in ensuring that those responsible for operating Canada's energy infrastructures have the intelligence, knowledge, and skills required to secure these vital systems against all threats.

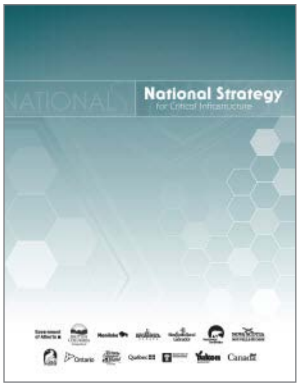
The National Energy Infrastructure Test Centre (NEITC) was established in 2012 with seed funding provided by Defence Research and Development Canada to fulfill Natural Resources Canada's (NRCan) legislative and policy obligations as the lead federal department for the energy and utilities sector.

Overseen by an industry-led advisory board, the NEITC collaborates with owners and operators to improve the security and resilience of Canada's critical energy infrastructure. The centre engages with energy sector organizations by providing assessments of the cyber-physical security of key facilities; evaluating and testing technologies; delivering knowledge transfer and skills development; and conducting research and development activities.

Canada's 10 critical infrastructure sectors



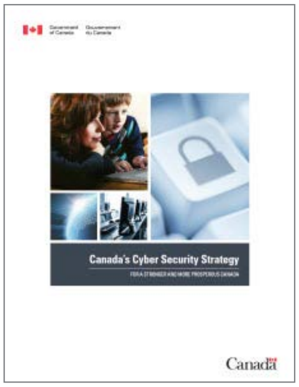
2. Policy context



The NEITC was established by NRCan in 2012 to help strengthen the security and resilience of Canada's critical energy infrastructures by leveraging trusted and collaborative relationships with energy sector partners.

Under the *Emergency Management Act* (2007), the *National Strategy for Critical Infrastructure* (2009), and the *Action Plan for Critical Infrastructure* (updated in 2014), NRCan is the designated lead federal department for the energy and utilities sector and has a mandate to:

- Build partnerships to support and enhance critical energy infrastructure resiliency.
- Implement an all-hazards approach to manage risk and emergencies.
- Advance timely information sharing among energy sector partners.

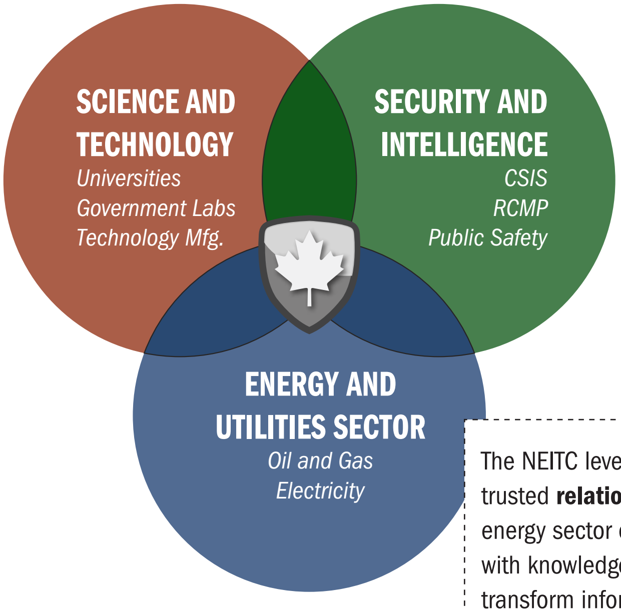

Canada's Cyber Security Strategy
FOR A STRONGER AND MORE PROSPEROUS CANADA
Canada

Canada's Cyber Security Strategy (2010) has three pillars: securing government systems; partnering to secure vital cyber systems outside the federal government; and helping Canadians to be secure online.

Under the partnering pillar, NRCan is called upon to leverage its partnerships and networks across the energy and utilities sector to enhance the cyber security of Canada's vital energy systems. Furthermore, *Action Plan 2010-2015* for *Canada's Cyber Security Strategy* identifies establishing the NEITC as a key deliverable.

The NEITC is important in helping NRCan and the Government of Canada to carry out their mandates by strengthening the links between the technology, security, and energy sector stakeholders. The centre occupies a unique position at the intersection of the Canadian critical infrastructure, security and intelligence community, and research institutions.

Canada's Energy Infrastructure Security Stakeholders



The NEITC leverages **expertise** and trusted **relationships** to provide energy sector owners and operators with knowledge and skills to transform information into **actions**.

3. Governance and collaboration

The NEITC was founded on the principal of **collaboration**. No single organization can be expected to have all the knowledge and expertise required to fully protect Canada's vital energy systems from a multitude of evolving threats. All NEITC engagement activities support industry's efforts in the secure operation of Canada's vast and diverse energy infrastructure.

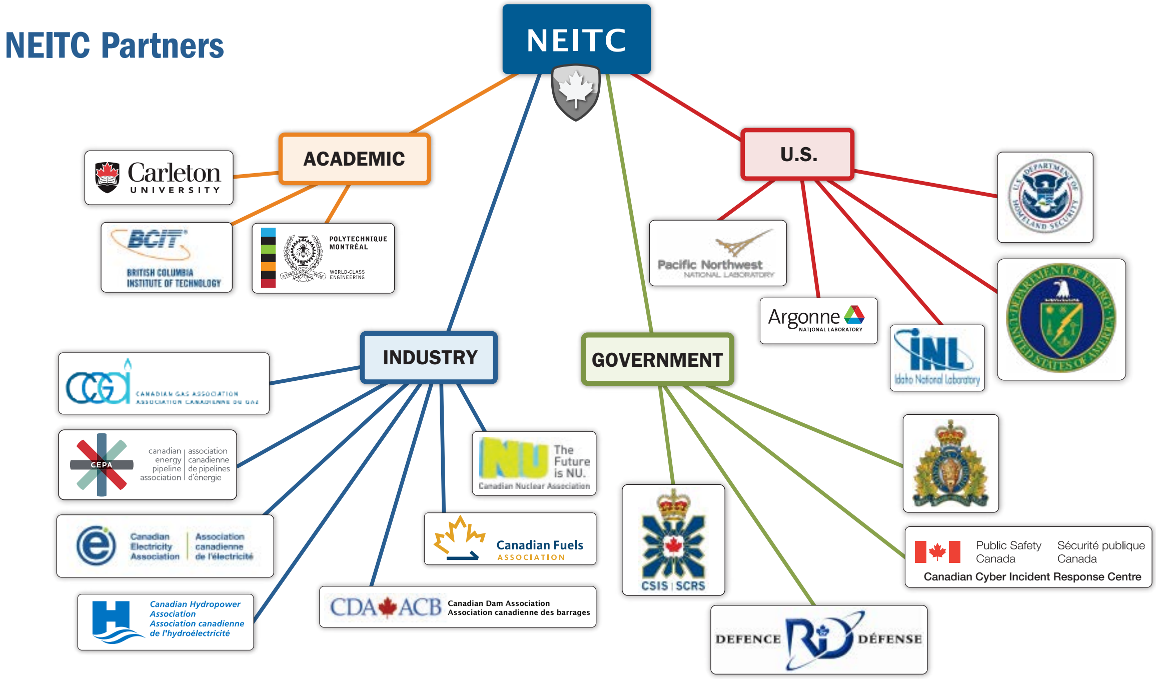
The centre's primary audience is the member companies of the **Energy and Utilities Sector Network** (EUSN). This national forum promotes the exchange of information and best practices among key energy stakeholders on critical infrastructure security. The EUSN convenes twice a year and is further supported by members who participate in four working groups:

- Strategy and Planning
- Societal Values / Forward Looking
- Security and Resiliency Research
- **NEITC Advisory Board**

The NEITC Advisory Board is drawn from a cross-section of EUSN members from across Canada's energy subsectors. This board helps to strengthen private-public partnerships, ensure that NEITC activities are relevant and provide value to infrastructure owners and operators. To help enhance the information-sharing process, a monthly EUSN-NEITC teleconference provides further engagement with energy infrastructure stakeholders.

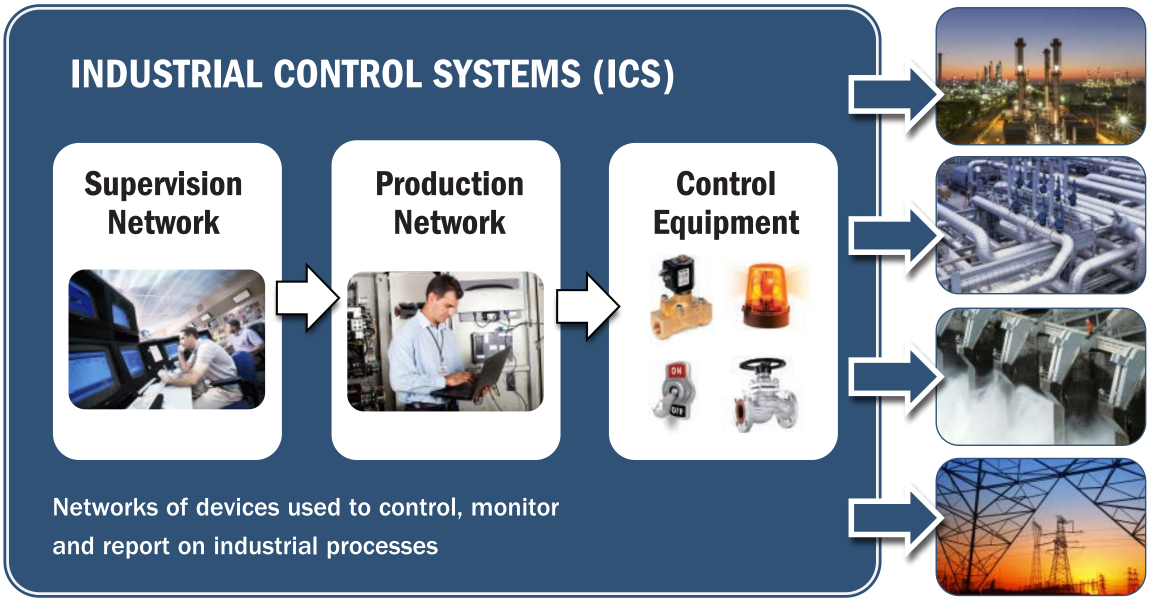
Agreements between the NEITC and the Canadian Cyber Incident Response Centre (CCIRC) and the Royal Canadian Mounted Police (RCMP) help to inform case studies and exercises and to streamline seamless government engagement with industry, thereby avoiding duplication of efforts.

Also, to enhance its own research efforts, the NEITC collaborates with Canadian and United States (U.S.) research institutions and government agencies on a variety of projects.


NEITC Partners
NEITC
ACADEMIC
Carleton University
BCIT British Columbia Institute of Technology
Polytechnique Montréal
INDUSTRY
Canadian Gas Association / Association canadienne du gaz
CEPA canadian energy pipeline association | association canadienne de pipelines d'énergie
Canadian Electricity Association | Association canadienne de l'électricité
Canadian Hydropower Association / Association canadienne de l'hydroélectricité
The Future is NU. Canadian Nuclear Association
Canadian Fuels Association
CDA ACB Canadian Dam Association / Association canadienne des barrages
GOVERNMENT
CSIS | SCRS
Defence R&D Défense
Public Safety Canada / Sécurité publique Canada
Canadian Cyber Incident Response Centre
U.S.
Pacific Northwest National Laboratory
Argonne National Laboratory
INL Idaho National Laboratory

4. Evolution of industrial control systems

Canada's critical energy infrastructure operates by using industrial control systems (ICS). An ICS uses hardware and software to manage and operate industrial processes and physical infrastructure, such as oil sand extraction, natural gas compression, and electrical co-generation power plants. Operators use an ICS to monitor or control each individual infrastructure element, such as circuit breakers, valves and pumps. These systems allow an operator to remotely open a valve on a pipeline or close an electrical breaker in the power grid with the click of a mouse.


INDUSTRIAL CONTROL SYSTEMS (ICS)
Supervision Network
Production Network
Control Equipment
ON
OFF
Networks of devices used to control, monitor and report on industrial processes

ICSs are not new; they have been used for years by engineers to effectively manage large and complex industrial processes and physical infrastructures. Historically, these functions were isolated from the business side of a company. Today, the drive for real-time business intelligence, cost-savings, and convenience has led to these vital systems being directly connected to corporate information technology (IT) networks and sometimes even connected to the Internet. This connectivity exposes ICSs to a vast array of cyber threats, which puts at risk the critical infrastructure that it manages. An attacker may take control of a pipeline, an electrical generator, or any ICS by "infecting" a control room operators' workstation. From there they could open and close valves or breakers to disrupt operations or destroy physical assets.

ICS TERMINOLOGY

IED –	intelligent electronic devices
SCADA –	supervisory control and data acquisition
DCS –	distributed control systems
PLC –	programmable logic controllers
HMI –	human machine interfaces
RTU –	remote terminal units

↑ Increased connectivity = ↑ Increased risk

5. Cyber threats

The energy and utilities sector must now deal with complex and evolving cyber threats, which include geo-politically motivated, state-sponsored security, intelligence and military units and their non-state proxies. Many of these state-sponsored threat actors have the resources and capabilities to run sophisticated corporate espionage operations and directly compromise ICSs.

Recent cyber-attacks on the energy sector

Baku–Tbilisi–Ceyhan Attack

- The oil pipeline exploded.
- Two people used laptops to exploit the security camera system to access the ICS.
- $1 billion in revenue was lost.

Shamoon Virus

- Saudi Aramco, the worlds' largest oil company, had 30,000 to 55,000 computers destroyed by the Shamoon virus.
- Qatar's RasGas company was also taken offline by the virus.

APT1

WANTED
BY THE FBI
Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets
Huang Zhenyu
Wen Xinyu
Sun Kailiang
Gu Chunhui
Wang Dong

- The state-sponsored group code named "APT1" is wanted by the FBI for economic espionage.
- The group is known to target the energy sector and ICSs.

Stuxnet

- The Stuxnet malware specifically targeted and damaged enrichment equipment at an Iranian nuclear facility.

Ukraine power outage

- Hackers caused a 2015 electricity outage in Ukraine by remotely switching breakers to cut power, after installing malware to prevent technicians from detecting the attack.

Bowman Avenue dam (New York, U.S.)

- An Iranian hacktivist group has claimed responsibility for a cyber-attack that gained control of a U.S. dam's flood gates in 2013.

Whether they are state-sponsored actors or low-level criminals, the Internet is increasingly the medium of choice for attackers because it is:

Inexpensive – Attackers do not need to travel, and many attack tools can be purchased for a modest price or downloaded for free from the Internet.

Easy – Attackers with only basic skills can cause significant damage if systems are not properly protected.

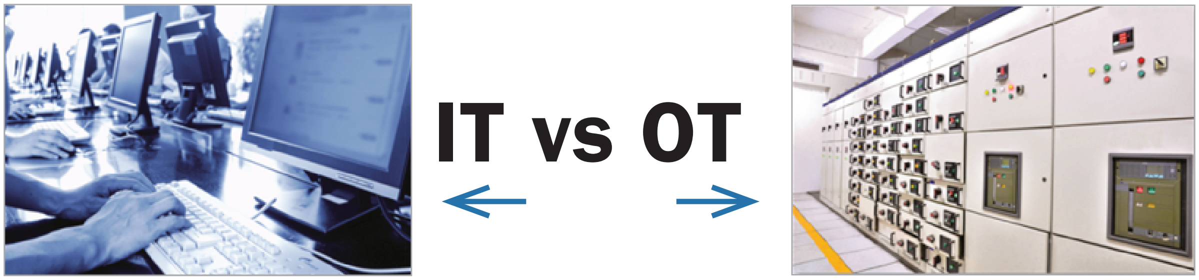
Effective – Even minor attacks can cause extensive damage to energy systems and/or create public embarrassment for the operators.

Low risk – Attackers can evade detection and prosecution by hiding their tracks through a complex web of computers and by exploiting gaps in domestic and international legal systems.

The NEITC aims to improve the security and resilience of Canada's critical energy infrastructures by helping owners and operators to address threats, identify vulnerabilities, and mitigate risks to their vital ICS. The centre has developed a unique expertise in ICS-related cyber security and leverages its access to high-value intelligence to address the cyber threats from sophisticated, state-sponsored actors. The NEITC works with the security and engineering teams of energy sector companies to implement strategies to mitigate an ever growing and evolving array of cyber threats.

6. Organizational challenges to security

Energy and utility companies face many organizational hurdles in their efforts to address the security and resilience challenges of their critical assets and operations. One of the key challenges to securing ICSs against cyber-attacks is the lack of clarity in the roles and responsibilities of the people responsible for securing both IT (e.g. corporate systems and email) and operational technology (OT) (i.e. ICS).



Information technology

Operational technology

For example, the chief operating officer (COO) is responsible to ensure that the company's operations run without interruptions. However, the security of the IT infrastructure required to run these operations falls under the purview of the chief information officer (CIO). This situation often creates confusion between control system engineers (who report to the COO) and IT personnel (who report to the CIO) about maintaining IT equipment in OT environments.

What is even more challenging is that OT engineers and IT personnel often disagree about patching vulnerabilities, updating anti-virus signatures, and installing monitoring agents. To the control system engineers, all changes to the IT equipment and settings can put operations at risk. Meanwhile, IT personnel view it a dangerous practice to run unpatched machines with out-of-date anti-virus signatures and without monitoring capabilities. These differences need to be resolved to maintain operations and secure IT equipment.

The NEITC offers a unique facility where energy and utility owners and operators can discover and address challenges ranging from a company's security culture to organizational structures to employee capabilities.

Common organizational challenges to ICS security and resilience	How the NEITC can help
Low “visibility” of security matters among senior executives	▪ Executive threat briefings and tabletop exercises
Limited resources and capabilities to detect and respond effectively to cyber-attacks	▪ Hands-on cyber exercises
Failure to identify vulnerabilities and security gaps in the ICS	▪ On-site security assessments
Inability to test and validate the ICS and cyber security technologies on their own systems without disrupting operations	▪ World-class test site that can reproduce a company’s IT and OT networks to evaluate new technologies before deployment
Limited knowledge of existing threats across the organization	▪ Cyber security awareness sessions

7. NEITC areas of strategic engagement

The NEITC delivers initiatives to improve the security and resilience of Canada’s vital energy systems. In particular, it collaborates with critical infrastructure owners and operators from the energy and utilities sector to identify security gaps and vulnerabilities in ICSs and to provide them with cost-effective solutions. The NEITC areas of engagement are divided into four broad categories.

Cyber-physical security assessments

- Security assessments help companies identify vulnerabilities and security gaps and inform companies about regulatory and policy compliance.
- A client company’s cyber-physical security is assessed by using:
  - penetration testing
  - vulnerability analysis and review
  - wireless security assessment
  - open source intelligence assessment
  - tabletop exercises

Technology testing

- New and existing ICS technologies are evaluated in a secure objective test environment. The NEITC team will provide recommendations and advice on ICS security implementations.
- The NEITC evaluates:
  - traditional and modern control systems
  - ICS configurations
  - industrial security features
  - energy sector-specific technology

Knowledge transfer and skills development

- Hands-on cyber exercises help front line responders, IT security personnel, and control system engineers to prevent, detect, respond to, and mitigate cyber-attacks.
- Sessions about cyber security awareness for managers, security personnel and engineers provide basic literacy in IT security, ICS technologies and cyber threats.
- Executive-level briefings explain the cyber threats to the energy and utilities sector.

Research and development

- The NEITC collaborates with various academic institutions to research and develop new technologies to improve the security and resilience of Canada's critical energy infrastructures. This work includes threat detection technologies that leverage advanced analytics and low cost sensors such as:
  - motion detectors
  - magnetic sensors
  - thermal imaging
  - chemical, oil and gas detection
  - gyroscopic sensors and accelerometers

8. Contact information

For questions or additional information, contact nrcan.neitc-cneie.rncan@canada.ca.

Part 2 NEITC strategic engagement areas

The following pages provide detailed descriptions of each NEITC strategic engagement area and how it provides value for the energy and utilities sector.

National Energy Infrastructure Test Centre

1. CYBER-PHYSICAL SECURITY ASSESSMENTS

The NEITC's cyber-physical security assessments meet both the operational security and regulatory and policy compliance needs of companies across the energy and utilities sector. The NEITC's assessment team uses its **security assessment framework** and leverages its relationship with the security, intelligence, and law enforcement community to provide a comprehensive assessment of a company's overall cyber security.

The assessment process leverages all available cyber intelligence to gain **cyber situational awareness** of the state of a client's IT and OT networks. The NEITC's assessment team works with client organizations to develop, implement, and test the tools, processes, and procedures required to maintain and update their security situational awareness as new intelligence emerges.

The NEITC's assessment team also leverages its state-of-the-art, world-class **cyber range**, which can reproduce real world energy infrastructures such as natural gas compression stations, oil sands processing operations, and electrical co-generation power stations. Using this unique capability, the team can replicate or emulate a client's IT and OT networks on its **secure**, stand-alone simulation network. The network is completely separate from both NRCan's corporate network and the Internet. By reproducing a client's IT and OT environments, the NEITC's assessment team can safely discover vulnerabilities and security gaps by using professional penetration testing tools and vulnerability scanners without putting the client's operations at risk.

TOP 3 operational assessment questions

- Who is responsible for IT security in the OT network?
- Who owns the IT equipment in the OT network?
- Who is monitoring your OT network?

The NEITC's security assessment methodology has a tiered two-phase approach. The first phase begins with the assessment team meeting senior management to set out the scope and objectives of the assessment. Once these are established, the team identifies key facility personnel, such as operators, control system engineers, and IT security personnel. The team works with these people to gather key documents for the assessment, such as security policies, business continuity plans, cyber incident response plans, and network diagrams. They will also interview key personnel to close any information gaps. After the data is gathered and analyzed, the client's overall security can be mapped against various standards, such as the NERC CIP 001-009, CSA Z246.1-09, and CSA N290.7.

COMPLIANCE ASSESSMENT STANDARDS (2016)

NERC CIP 001-009	Cyber security standards on elements related to critical infrastructure developed by the North American Electric Reliability Corporation (NERC).
CSA Z246.1	Performance-based security management standards for the petroleum and natural gas industry.
CSA N290.7	Cyber security for nuclear power plants and small reactor facilities.

The second phase of the cyber-physical security assessments is to validate through technical means key assumptions and findings from the first phase of the process. The validation is done to guarantee to a high level of assurance that compliance is actually met, and not just "on paper." To accomplish this, NEITC's team provides an array of additional services, such as vulnerability scanning, penetration testing, and validation testing. Each of these services can verify different aspects of compliance to obtain a complete picture of the client's overall security.

Vulnerability assessment

A vulnerability assessment is the process used to discover security "holes" from unpatched software, libraries, and operation systems. It is a compulsory component in multiple compliance standards, including under NERC CIP-005 and CIP-007. Unfortunately, conducting vulnerability assessments on live OT networks can put a company's production operations at risk. The NEITC leverages its state-of-the-art cyber range technology to solve this problem. With its unique capabilities, we reproduce an organization's operational network and perform extensive testing on it to **safely** discover vulnerabilities and security gaps in the production environment. This "off-line" vulnerability assessment is complemented by validating the results by passively collecting information on the operational network, which does not put a client's production and operations at risk.

Penetration testing

Penetration testing involves running a “scripted” cyber operation against a client’s organization under controlled conditions. The NEITC’s team can reproduce real world cyber-attacks from sophisticated state-sponsored actors against an organization’s corporate IT network and operational production systems. By simulating an adversary, such as a hostile foreign intelligence agency running an espionage operation, the company’s executives can gain a better understanding of the real risks that they face.

A penetration test can **quantitatively** assess the effectiveness of the security measures and processes that have been put into place to prevent such cyber threats from stealing valuable intellectual property or compromising vital operational ICS networks. The result of a penetration test is identifting weaknesses in an organization’s security before a real adversary exploits them. The test allows a client to identify security gaps in the people, processes, and technologies used to protect its business.

Wireless security assessment

Today, cyber criminals and spies can leverage an organization’s wireless infrastructure to break into a company network to steal sensitive documents, or worse, to gain access or control of its operational production network. They can exploit access point misconfigurations, weak encryption, and “signal bleed” to get into a company’s corporate network before moving on to their operations. A security assessment of a client company’s Wi-Fi network infrastructure has become an essential part of any security assessment.

A wireless assessment includes discovering all Wi-Fi network access points (i.e. hotspots), evaluating the encryption scheme used for over-the-air data transmission, and determining how far the wireless signal extends beyond its intended perimeter. This exercise is supplemented with wireless penetration testing to identify the various pathways that an adversary can exploit to compromise an organization’s network. In addition, all use of Wi-Fi technologies in OT environments is assessed for possible risks to critical operations.

Open source intelligence assessment

Open source intelligence (OSINT) assessments consist of gathering and analyzing publicly available information about a client’s company. This is information that can be found on the Internet, the Deep Web, or the Dark Web but does not involve any type of “hacking.” In today’s global, interconnected world, companies regularly find that internal corporate documents have found their way onto the World Wide Web. Moreover, company employees can accidentally reveal sensitive company information on one of a multitude of social media platforms. OSINT can be used to assess an organization’s public information exposure through the use of advanced tools and techniques to gather from all possible sources of information relevant to the company. Any comprehensive security assessment of a company should include OSINT.

Tabletop exercises

A comprehensive security assessment must evaluate an organization's plans for how to respond to incidents and emergencies and how to ensure business continuity. The most cost-effective way to assess each of these plans is to perform comprehensive tabletop exercises. By working through various scenarios with the key personnel responsible for implementing each of these plans, one can identify procedural weaknesses and gaps that could compromise the effectiveness of the planned response. The NEITC's assessment team has extensive experience developing cyber scenarios for tabletop exercises to evaluate various plans, including cyber incident response plans. Each of the scenario-based exercises can be effectively administered in a three-hour session at a client site.

The NEITC offers cyber-physical security assessments, knowledge transfer and skills development, technology testing, and research and development services tailored to Canada's energy and utilities sector.

NRCAN.NEITC-CNEIE.RNCAN@CANADA.CA

National Energy Infrastructure Test Centre

2. TECHNOLOGY TESTING

What ICS equipment is secure?

Does it perform to specifications?

The NEITC offers an objective testing facility for new and existing ICS equipment to identify vulnerabilities and assess their security implications prior to deployment.

ICS technology is evolving to include Internet connectivity for its components. In the pursuit of more reliable, capable and efficient operations, energy infrastructure owners and operators may be unknowingly exposing themselves to security vulnerabilities that can be exploited. Since the primary focus of vendors, operators, and engineers is to ensure the continued functionality of systems, security often becomes an afterthought. Another weakness is that commercial IT security solutions that can be bought off-the-shelf protect only corporate networks, not ICS equipment. The Stuxnet targeting of Iranian systems is a prime example of the potential consequences of a vulnerable ICS.

The NEITC offers objective and reliable assessments of technologies. A multidisciplinary team of subject matter experts performs clear and accurate testing. They use a multi-layered methodology to analyze technologies through several phases of testing. Leveraging academic, industrial, and government partners, the NEITC continually incorporates cutting-edge techniques and procedures into its testing process. Security vulnerabilities are analyzed at all layers of a system, including communications, software, hardware, and design. Device functionality is verified during each testing phase. Advanced test benches for energy sector systems are used to establish performance metrics for each device under test to ensure reliable and repeatable test methodologies are followed.

The NEITC evaluates:

- traditional and modern control systems
- ICS configurations
- industrial security features
- energy sector-specific technology

Survey of ICS professionals

34% believe their systems have been breached more than twice in the past 12 months.

42% see external actors as the No. 1 threat vector.

SANS Institute, *The State of Security in Control Systems Today*, June 2015

TECHNOLOGY

- embedded devices (PLC, IED)
- monitoring (sensors)
- networked devices (SCADA, protocols)
- security appliances
- valves, relays, other industrial hardware
- pumps, generators, transformers

VECTORS OF ATTACK

- misconfiguration of devices
- malformed packet handling
- denial of service
- unknown third-party components
- protocol and communication networks
- design faults
- removable media

TESTING METHODOLOGIES

- scenario validation
- hardware functionality review
- test and monitor
- protocol analysis
- optimizing configuration settings

The NEITC's independent technology testing replicates real world conditions in a simulated environment to enhance the reliability of an ICS. Customized recommendations and analysis are provided for each tested device or system. ICS operators stand to benefit from ↓**reduced risks**, ↓**reduced costs**, and ↓**reduced downtime**.

The NEITC offers cyber-physical security assessments, knowledge transfer and skills development, technology testing, and research and development services tailored to Canada's energy and utilities sector.

NRCAN.NEITC-CNEIE.RNCAN@CANADA.CA

3. KNOWLEDGE TRANSFER AND SKILLS DEVELOPMENT

Securing an ICS from cyber threats is a growing challenge. Over the past 20 years, ICSs has evolved from "in-house," custom-built engineering systems to commercial, off-the-shelf solutions that can run on standard IT equipment. These systems that used to run in isolation are now being connected to corporate IT networks and sometimes even to the Internet.

These fundamental changes to the operational environments for ICSs have exposed them to all the cyber threats that affect conventional IT networks. Unfortunately, the cyber security solutions that have been developed for corporate IT networks are not well-suited for OT systems. Some of these security technologies can put ICS operations at risk by blocking legitimate communications that were mislabelled as suspicious or by deleting engineering files mistakenly tagged as malicious. Cyber security in OT networks requires that IT security professionals and control system engineers understand the risks associated with each of these technologies and how to safely use them in their operations.

To address these and other problems faced by industry, the NEITC offers **knowledge transfer and skills development sessions**. In particular, it delivers hands-on cyber exercises designed specifically to answer the challenges of securing OT networks by using conventional IT security technologies. These exercises provide a unique opportunity to acquire essential knowledge for securing ICS networks and to gain practical experience using cyber security technologies in operational environments. The training is suitable for incident responders, IT security personnel, control system engineers, and network architects. The trainees also receive a detailed picture of the current cyber threats that the energy and utilities sector faces and an in-depth look at the tools, techniques, and procedures for defending against advanced persistent threats (APT). Since 2012, the NEITC has trained about 140 industry professionals.

Hands-on skills development

- attacker life-cycle process
- intelligence life-cycle process
- using indicators of compromise (IOC)
- blacklisting vs. whitelisting technologies
- building intrusion detection and prevention rules
- reverse engineering covert channels
- understanding IT vs. OT networks
- fingerprinting ICS traffic flows
- **Red team** vs. **Blue team** exercises

Target audience

- **IT security professionals**
- **control system engineers**
- **network architects and engineers**
- **incident responders**

THE NEITC CURRICULUM

INTRODUCTORY LEVEL: Understanding the strategic implications of cyber threats: From IT to ICS

The participants will learn the strategic implications of cyber threats to a company's operational environment. In particular, they will learn about recent cyber espionage campaigns that are targeting Canada's energy sector and will be given an in-depth look at the tradecraft used by APTs through live demonstrations and hands-on exercises.

The trainers will explain how Canada's security, intelligence, and law enforcement community provides cyber-related intelligence to industry to detect sophisticated cyber threats. The participants will learn how to effectively perform the intelligence life-cycle process and leverage IoCs to detect, contain, and eradicate targeted cyber-attacks from APTs. They will also learn the basics about ICS technologies and the key differences between them and conventional IT systems.

Finally, the participants will practice using the knowledge and skills acquired in the first three days in a **Red team** vs. **Blue team** exercise that will test their ability to defend an ICS network against targeted cyber-attacks. The participants will be required to identify network breaches using IoCs, perform the intelligence life-cycle process to track down the adversary, utilize cyber-related intelligence to determine the nature of the threats, and prepare briefings for their senior management. **(4 days)**

INTERMEDIATE LEVEL: Detecting and responding to cyber-attacks: From IT to ICS

Participants will learn to efficiently detect and respond to sophisticated cyber-attacks against IT and OT networks. Trainees will learn, through a series of hands-on exercises, how to effectively identify compromised hosts, track an adversary's movement across IT and ICS networks, and terminate an APT cyber operation at the network level.

The trainers will expose the latest tools, techniques and procedures used by sophisticated cyber threat actors to compromise an organization's network through live demonstrations and hands-on exercises. Participants will learn how to use various technologies as effective security analysis tools, including *SysInternals, Wireshark* and *Snort*.

The trainees will use these technologies to identify malicious processes running on a host and covert communications. They will also practice how to reverse engineer covert channels used by APTs and producing rules for blacklisting intrusion detection systems (IDS).

Finally, the participants will practice using the knowledge and skills acquired in the first three days in a **Red team** vs. **Blue team** exercise. The exercise will test their ability to detect and respond to targeted cyber-attacks from APTs against IT and ICS networks. Participants will be required to identify infected computers through host-level analysis, uncover covert communication channels, produce blacklisting IDS rules, determine the nature of the threat, and provide senior management with briefings and recommendations. **(4 days)**

ADVANCED LEVEL: Preventing and investigating cyber-attacks: From IT to ICS

Participants will learn to prevent cyber-attacks against OT networks and investigate cyber intrusions into IT networks from APTs. In particular, they will learn advanced state-of-the-art techniques to design, configure, and monitor ICSs to prevent cyber-attacks from compromising operational networks. They will also learn, through a series of hands-on exercises, how to effectively collect forensic evidence left by sophisticated threat actors in order to reconstruct an espionage operation.

The trainees will practice using tools and technologies such as *TShark, Scapy,* and *Python*. They will analyze ICS network traffic, produce a fingerprint for ICS traffic flows, and generate rules for whitelisting intrusion prevention systems (IPS) to block malicious packets at the network level. Trainees will also complete exercises in which they will build, deploy, and validate the effectiveness of their custom-configured IPS to block cyber-attacks targeting an ICS.

Finally, the participants will practice using the knowledge and skills acquired in the first three days in a **Red team** vs. **Blue team** exercise. The exercise will test their ability to prevent an OT network from being compromised and investigate network breaches into the corporate IT networks. Participants will be required to re-architect IT and OT networks, deploy sensors across these networks, produce blacklisting and whitelisting IDS and IPS rules, investigative a cyber intrusion in the corporate IT network, determine the nature of the threat, and brief senior management on a potential espionage operation. **(4 days)**

These hands-on training and exercise sessions offer a unique opportunity to gain practical real world experience to prevent, detect, respond to, and investigate targeted cyber-attacks against IT and OT environments from sophisticated threat actors. These sessions provide an environment where trainees can practice using the tools, techniques, technologies, and processes taught by the trainers. This is done through a series of hands-on exercises in small teams of two to three people, in which each team is provided their own "ICS Sandbox" on the NEITC's cyber range. The training sessions end with a full-day "live fire" team exercise (e.g. **Red team** vs. **Blue team**) to solidify the new knowledge and skills.

CYBER AWARENESS: Executive threat briefing and awareness sessions

Many of the obstacles that companies face to secure operational environments against cyber-attacks are not technical in nature but rather organizational challenges. In particular, there is often a lack of buy in among senior executives to put the right people, processes, and technologies in place to protect business operations. Additionally, operational managers and security personnel may be unaware of vulnerabilities, threats, and risks facing their ICS. To address these challenges, the NEITC provides on-site executive threat briefings for senior leadership and general cyber security awareness training for managers, engineers, and security personnel.

Quotes from industry trainees

"... learned great skills"

"Instructors were great!"

"I think this course should be mandatory for all owners of an ICS in Critical Infrastructure."

"Great opportunity to train with others in the industry"

"Unique and needed training opportunity"

"The government should be spreading this message far and wide and [the NEITC] team are well equipped to do this"

The NEITC offers cyber-physical security assessments, knowledge transfer and skills development, technology testing, and research and development services tailored to Canada's energy and utilities sector.

NRCAN.NEITC-CNEIE.RNCAN@CANADA.CA

National Energy Infrastructure Test Centre

4. RESEARCH AND DEVELOPMENT

Toward resilient energy infrastructure

Canada's vital energy systems encompass thousands of kilometres of powerlines, pipelines, and gas distribution networks that transport energy from remote production locations to our towns and cities. This vast and diverse infrastructure creates a dynamic and challenging security landscape. Energy sector owners and operators are responsible to protect their assets from a variety of threats ranging from aging infrastructure to natural hazards to human-induced damage, whether criminal or unintentional. Because the energy sector is critical to the economy, recent failures have caused billions of dollars in damages and economic impacts.

re·sil·ience

(n.) the capacity to recover quickly from difficulties; toughness

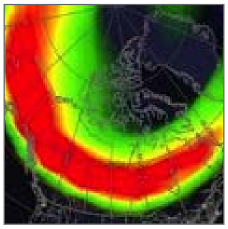
Natural hazards

Theft/tampering

Cyber-attacks

Sabotage

Solar storms



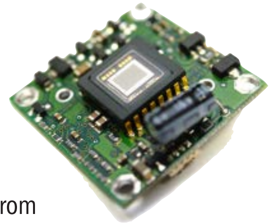
A resilient organization is one that can quickly detect incidents, mitigate the effects of existing threats, and rapidly restore operations after incidents have occurred. A key to improving the energy sector's security and resiliency to all hazards is **technological advancement**. Research at the NEITC in cooperation with industry, government, and academic institutions gives the NEITC the unique advantage of wide and interdisciplinary approaches to address critical infrastructure vulnerabilities.

Sensors and data analytics

Research and development of sensors and analytics advance infrastructure resilience by increasing our knowledge of security technology that is highly effective, low-cost, and easily deployable. There have been many developments in sensor systems and in distributed computing systems that are portable and miniature, as well as many applications of these advancements in other sectors.

Fixed and mobile sensors can be used in a variety of security and response implementations. The miniaturization of components has led to the broadening of technological applications while reducing the overall cost. By properly collecting and analyzing the data from sensors, organizations can more effectively and efficiently detect and prevent potential threats, as well as respond to and recover from events in progress. Greater situational awareness about active threats will allow operators and authorities to improve allocation of resources and response times.

Examples of sensors and applications:



Motion detection: Can detect and deter unauthorized entry, theft or vandalism.

Magnetism: Can detect electromagnetic anomalies, such as cell phones or laptops to help determine if disturbances stem from human activity.

Thermal imaging: Can be used to detect anomalies, such as temperature variations stemming from leaks in pipelines.

Chemical, oil and gas detection: Can help detect and monitor leaks and spills and help to prevent explosions by detecting fuel mixtures.

Gyroscopic sensors: Can quickly determine if electrical towers in remote locations have been damaged by measuring tilt and acceleration.

Sensor data fusion is a powerful method of combining the data from a variety of sources (such as those in the previous list) to provide better awareness and response. Sensors and data analytics provide the means to produce operational intelligence for owners and operators of critical infrastructure, thus reducing risks and costs. Data fusion involves both collecting the data and developing the algorithms to categorize and classify the data. The goal is to increase situational awareness and thereby enable unique and strategic approaches and responses to emerging threats.

Unmanned aerial vehicles

Unmanned aerial vehicles (UAV) are being used with a suite of sensors that can detect visual, auditory, chemical and other metrics. Adding UAVs to the strategic response plan increases the monitoring capability of owners and operators, thereby helping the surveillance of these vastly distributed networks of interconnected components. UAVs offer enhanced coordination with sensors on the ground and with first responders. UAVs also are less impacted by physical barriers than most sensors, and thus can provide operational intelligence during an emerging threat such as a natural disaster.

Research partnerships

The NEITC is continually expanding its research portfolio to develop knowledge and value-added technology for the benefit of the energy and utilities sector. Their research partnerships with industry and academia include:

- **École Polytechnique de Montréal:** access control and cyber security
- **British Columbia Institute of Technology:** micro-grids
- **Carleton University:** sensors and data analytics
- **NRCan's Geomagnetic Laboratory:** impacts of space weather

The NEITC offers cyber-physical security assessments, knowledge transfer and skills development, technology testing, and research and development services tailored to Canada's energy and utilities sector.

NRCAN.NEITC-CNEIE.RNCAN@CANADA.CA

Invitation to collaborate with the NEITC

Every company has unique processes, threats, and requirements. The NEITC will collaborate with you to develop a tailored package of initiatives to help your organization address its security and resilience challenges. The centre currently operates under a partial cost-recovery model and makes every attempt to keep costs at a minimum. Contact the NEITC to learn how you can:

- Receive an objective and comprehensive security assessment.
- Test new technology before implementation.
- Provide cyber training to employees.
- Partner with NRCan to conduct research and/or participate in field deployment tests.

✉ **NRCAN.NEITC-CNEIE.RNCAN@CANADA.CA**