Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

National Energy Infrastructure Test Centre (NEITC)

Concept and Development of an Entity to Assist in Cyber Protection of Industrial Control Systems within the Energy and Utilities Sector in Canada

Rodney Howes
Defence R&D Canada – Centre for Security Science

Douglas Hales
D Hales Consulting Inc.

Dr. Andrew Vallerand
Defence R&D Canada – Centre for Security Science

Defence R&D Canada – CSS

Technical Memorandum
DRDC CSS TM 2013-055
March 2014

Canada

National Energy Infrastructure Test Centre (NEITC)

Concept and Development of an Entity to Assist in Cyber Protection of Industrial Control Systems within the Energy and Utilities Sector in Canada

Rodney Howes
Defence R&D Canada – Centre for Security Science

Douglas Hales
D Hales Consulting Inc.

Dr. Andrew Vallerand
Defence R&D Canada – Centre for Security Science

Defence R&D Canada – CSS

Technical Memorandum
DRDC CSS TM 2013-055
March 2014

This work was supported by the Canadian Safety and Security Program which is managed by the Defence Research and Development Canada – Centre for Security Science.

The authors would like to acknowledge the contributions of Federal and private sector partners who have and continue to contribute to realization of a NEITC. The efforts of Public Safety (the Canadian Cyber Incident Response Centre), Natural Resources Canada, the Royal Canadian Mounted Police and the Canadian Security Intelligence Service in particular deserve to be singled out.

Abstract

Awareness of the vulnerability of SCADA and ICS networks increased dramatically following exposure of the 2010 *Stuxnet* virus which targeted Iran's nuclear facilities. This was the first publicly known attack on a programmable logic controller and highlighted the need for better testing and monitoring capabilities and more effective collaboration and training. Risk precludes using "live" systems; hence, an independent, complementary capability was needed. A requirement to integrate digital and physical components of SCADA and ICS systems and an opportunity to exploit emulation and simulation were identified. The concept of a "sandbox" used by software programmers to run untested code or untrusted programs in isolation was adopted. Several Federal partners collaborated to create an ICS test and training centre. This report summarizes key elements of the concept and development of the nascent National Energy Infrastructure Test Center (NEITC).

Résumé

La découverte en 2010 du virus Stuxnet, qui ciblait des installations nucléaires en Iran, a révélé les graves lacunes que présentent les réseaux de systèmes de contrôle et d'acquisition de données (SCADA) et les réseaux de systèmes de contrôle de processus (SCI). Première attaque divulguée au public, elle visait un contrôleur logique programmable et a mis en évidence la nécessité de disposer de meilleures capacités d'essai et de surveillance, ainsi que d'une collaboration et d'une formation plus efficaces pour contrer un tel problème. Comme l'utilisation de systèmes opérationnels présente trop de risques, il fallait donc recourir à une capacité complémentaire et indépendante. On a constaté que les composantes numériques et physiques des systèmes SCADA et SCI devaient être intégrées, et qu'on avait là l'occasion de tirer parti des technologies d'émulation et de simulation. On a alors adopté le principe du « bac de sable » que les programmeurs appliquent en milieu isolé lorsqu'ils exécutent du code ou des programmes non testés. Plusieurs partenaires fédéraux ont participé à la mise sur pied d'un centre d'essai et de formation sur les SCI. Le présent rapport résume les éléments clés du concept et de l'établissement du nouveau Centre national d'essai de l'infrastructure énergétique (CNEIE).

Executive Summary

National Energy Infrastructure Test Centre (NEITC): Concept and Development of an Entity to Assist in Cyber Protection of Industrial Control Systems within the Energy and Utilities Sector in Canada

Rodney Howes, Doug Hales and Andrew Vallerand; DRDC CSS TM 2013-055; Defence R&D Canada – CSS; March 2014.

Introduction or background: Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems were not designed with security foremost in mind, and the adoption of standard interfaces and communication protocols and connectivity to open networks ("deperimeterization") and integration into corporate business networks has dramatically increased their exposure and vulnerability to error and/or attack. A number of "attacks" have highlighted the requirement to address cyber resiliency related concerns. Security challenges now extend from power generation to distribution. The traditional electrical power grid is currently transforming into a "Smart Grid", an integrated network that relies on digital and advanced technologies to monitor and manage in real time the transmission and distribution of electricity from generation sources to end users. Smart Grids face exposure to the threats SCADA systems face. Pervasive digitalization and increasing societal and economic reliance renders assurance and cyber reliance a collective responsibility.

The National Energy Infrastructure Test Centre (NEITC) originated as a concept, prompted by the need to inspire and coordinate a response to this increasing threat. Six potential roles ranging from sponsoring research to testing equipment and determining best practices through to hosting workshops and conducting courses to organizing on-site assessments were identified. In a rapidly changing environment, such as cyber security, there are particularly good reasons for coupling practice and training.

Results: The NEITC has progressed from concept to capability. First steps involved establishing partnering arrangements inside government and leveraging existing networks and associations in the energy and utilities sector. A comprehensive threat assessment was commissioned providing a common departure point. Subsequently, a governance structure reflecting public/private collaboration was established to socialize and champion the concept and provide direction. Natural Resources Canada (NRCan) generously offered space and equipment was donated and fitted to create a functioning laboratory capable of supporting testing and training. An emulation capability and control room were added permitting training to be conducted. Initial operating capability was achieved in March 2013 and an initial course held that month. A second course was held in November 2013 and a third is planned for March 2014. A questionnaire conducted following the inaugural course affirmed requirements and the need for a NEITC.

Significance:

This program, implemented as suite of projects, provides a number of lessons. Engagement began with a community-driven threat assessment which helped established a baseline, a common appreciation of challenges. The post-harmonization CSSP integrates demand (call for proposal)

and supply (targeted investments) driven approaches and also accommodates sponsorship of community development initiatives. "Projectizing" development of the NEITC facilitated management and allowed for review and adjustment. This flexibility ensured that S&T remained in lock-step with ICS/SCADA practitioners.

The notion of designing an environment in which factors can be controlled and experiments conducted is not new. Creation of a sandbox (nomenclature derived from the field of software programming) reflects an extrapolation of the concept. It appears to be exceptionally well suited to many aspects of cyber security such as ICS/SCADA and Smart Grid where technology is evolving rapidly and the risk to systems and services preclude operational testing. This program has reinforced the utility of the concept and pointed to a central and critical contribution that CSS can make, a role directed more to facilitating and empowering communities of practice than to anticipating and stipulating products.

Future plans: Key partners have co-invested to create a "sandbox", an ecosystem capable of supporting research and training and seen to contribute value to SCADA security to owners and operators in the energy and utilities sector. Next steps involve enriching and formalizing coursing, developing site assessments protocols and practices, and investigating options for institutionalization and transition to self-sustainment. Expansion to include Smart Grid is being examined and, as a first step, a workshop was recently (January 2014) conducted in Vancouver. Smart Grid confronts many challenges that ICS/SCADA owners and operators have met and are facing. In light of these parallels and technological convergence, thought is being be given to expanding the scope of a NEITC, creating a testing and training environment to support end-to-end power generation and distribution. The sandbox concept is now being applied to CSSP-2013-TI-1045 Canadian National Cyber Forensics Capability. A collaborative partnership with the National Cyber Forensics Training Alliance (NCFTA), a Pittsburgh-based not-for-profit, has been set up which will enable Canadian stakeholders, public and private, to establish information sharing protocols and collectively determine the way forward to detect identify, mitigate and neutralize cyber threats. Meanwhile a fledgling collaboration continues apace and the NEITC is up, running and evolving.

Sommaire

National Energy Infrastructure Test Centre (NEITC): Concept and Development of an Entity to Assist in Cyber Protection of Industrial Control Systems within the Energy and Utilities Sector in Canada

Rodney Howes, Doug Hales and Andrew Vallerand; DRDC CSS TM 2013-055;

R & D pour la défense Canada – CSS; Mars 2014.

Introduction : Les systèmes SCADA et SCI n'ont pas été conçus avant tout pour répondre à des impératifs de sécurité. L'adoption d'interfaces et de protocoles de communication normalisés et d'une connectivité avec des réseaux ouverts (élimination du périmètre), ainsi que leur intégration aux réseaux d'entreprise, ont considérablement augmenté le niveau d'exposition et de vulnérabilité aux erreurs et aux attaques de ces systèmes. Des attaques ont mis en évidence la nécessité de chercher des solutions aux problèmes en lien avec la résilience cybernétique. Les obstacles à la sécurité s'étendent maintenant aux systèmes de production et de distribution d'électricité. Les réseaux électriques traditionnels deviennent « intelligents », c'est-à-dire des réseaux intégrés exploitant des technologies numériques de pointe pour surveiller et gérer en temps réel le transport et la distribution d'électricité, des sources de production jusqu'aux consommateurs. Ces réseaux intelligents font face aux mêmes menaces que les réseaux SCADA. Leur numérisation omniprésente, alliée à une dépendance accrue de l'économie et de la société à leur égard, font de la fiabilité cybernétique et de l'assurance une responsabilité collective.

Le Centre national d'essai de l'infrastructure énergétique (CNEIE) a été mis sur pied pour contrer une menace cybernétique grandissante et coordonner les interventions en ce sens. Il est appelé à tenir six rôles possibles, soit le parrainage de projets de recherche, la réalisation d'essais de matériel, l'établissement de pratiques exemplaires, la tenue d'ateliers et de séances de formation et l'organisation d'évaluations sur place. Dans un environnement qui évolue rapidement, tel celui de la sécurité cybernétique, il y a lieu de joindre la pratique et la formation.

Résultats : Au départ un simple concept, le CNEIE est devenu une capacité. Les premières étapes de sa concrétisation ont consisté à établir des accords de partenariat à l'intérieur du gouvernement et à tirer profit des réseaux et des associations existants dans le secteur de l'énergie et des services publics. Une évaluation exhaustive des menaces a été commandée pour servir de point de départ commun. Par la suite, on a mis en place une structure de gouvernance à l'image de la collaboration entre secteurs privé et public en vue de faire connaître et de promouvoir le Centre et lui donner une orientation. Les locaux offerts gracieusement par Ressources naturelles Canada (RNCan) et du matériel spécialement adapté obtenu gratuitement ont permis de créer un laboratoire fonctionnel où l'on peut effectuer des essais et donner de la formation. À ce dernier chapitre, on a ajouté au Centre une capacité d'émulation et une salle de

contrôle. C'est en mars 2013 que le Centre est devenu opérationnel et que le premier cours a été dispensé. Le deuxième cours a été donné en novembre 2013, et un troisième est prévu en mars 2014. Les résultats d'un questionnaire distribué à la suite du premier cours ont permis de confirmer que le CNEIE répond à un besoin réel.

Importance : Le programme du CNEIE, mis en œuvre sous la forme d'une série de projets, a permis de tirer plusieurs leçons. La mobilisation a débuté par une évaluation des menaces axée sur la communauté afin d'établir une base de référence, une appréciation commune des défis à relever. Le Programme des études de sécurité canadienne (PESC) après l'harmonisation intègre les approches axées sur la demande (appel de propositions) et l'approvisionnement (investissements ciblés), en plus de favoriser le parrainage d'initiatives de développement communautaire. Le développement par projets du CNEIE a facilité le travail de gestion et permis de procéder à des examens pour rectifier le tir. Une telle souplesse a fait en sorte que le secteur de la S & T a pu collaborer étroitement avec les praticiens des réseaux SCI et SCADA.

L'idée de concevoir un environnement dans lequel il est possible de réaliser des expériences et de contrôler des facteurs n'a rien de nouveau. La création d'un bac de sable (une nomenclature qui existe déjà dans le domaine de la programmation de logiciels) reflète une extrapolation du concept. Elle semble exceptionnellement bien adaptée à bien des aspects de la sécurité cybernétique, comme les réseaux SCI, SCADA et intelligents, où la technologie se transforme rapidement et où les risques auxquels les systèmes et les services sont exposés empêchent de procéder à des essais opérationnels. Le PESC a démontré l'utilité indiscutable du concept et souligné la contribution à la fois centrale et essentielle des études de sécurité canadiennes, un rôle davantage axé sur l'aide aux communautés de pratique et sur leur habilitation, que sur l'attente de produits et sur l'établissement de leurs spécifications.

Projets futurs : Des partenaires clés ont investi conjointement afin de créer un bac de sable, un écosystème capable d'appuyer la recherche et la formation, qui confère plus de sécurité aux réseaux SCADA aux yeux des propriétaires et des exploitants du secteur de l'énergie et des services publics. Les prochaines étapes consisteront à étendre et à formaliser le contenu des cours, à élaborer des protocoles et des pratiques d'évaluation des sites et à envisager la possibilité de créer des établissements et d'opérer une transition vers l'autonomie. On envisage à l'heure actuelle d'étendre la portée aux réseaux intelligents. Un premier atelier a été tenu récemment (en janvier 2014) à Vancouver. Les réseaux intelligents présentent de nombreux défis que les propriétaires et les opérateurs de réseaux SCADA et SCI doivent ou ont dû relever. À la lumière de ces parallèles et de la convergence technologique, on a pensé étendre la portée du CNEIE pour créer un environnement d'essai et de formation en vue d'appuyer la production et la distribution d'électricité. Le concept de bac de sable est maintenant appliqué à la capacité nationale d'intervention judiciaire contre la cybercriminalité du Canada (CSSP-2013-TI-1045). Un partenariat de collaboration a été établi avec la National Cyber Forensics Training Alliance

(NCFTA), une société américaine à but non lucratif de Pittsburgh. Une telle association permettra aux intervenants canadiens des secteurs privé et public de mettre en place des protocoles de partage de renseignements et de définir ensemble la marche à suivre pour détecter, identifier, atténuer et neutraliser les menaces cybernétiques. Dans l'intervalle, cette toute nouvelle collaboration se poursuit, et le Centre national d'essai de l'infrastructure énergétique est entièrement opérationnel et poursuit son évolution.

Table of contents

List of figures

List of tables

.

1 Introduction

1.1 Threat/Hazard Environment

> *Control computers were built to run behind the safety of brick walls. But such security is rapidly being eroded by links to the Internet*[1]

How can Canada protect the cyberspace of our country, without restricting the open flow of information on the internet? The present state of security for Supervisory Control and Data Acquisition (SCADA) systems is not commensurate with the constantly growing and evolving threat or potential consequences of such threats. SCADA systems were not designed with security foremost in mind and the adoption of standard interfaces and communication protocols and connectivity to open networks (not least the Internet) and integration into corporate business networks has dramatically increased exposure and vulnerability to error and/or attack.

> Initially, ICS had little resemblance to traditional information technology (IT) systems in that ICS were isolated systems running proprietary control protocols using specialized hardware and software. Widely available, low-cost Internet Protocol (IP) devices are now replacing proprietary solutions, which increases the possibility of cyber security vulnerabilities and incidents. As ICS are adopting IT solutions to promote corporate business systems connectivity and remote access capabilities, and are being designed and implemented using industry standard computers, operating systems (OS) and network protocols, they are starting to resemble IT systems. This integration supports new IT capabilities, but it provides significantly less isolation for ICS from the outside world than predecessor systems, creating a greater need to secure these systems. While security solutions have been designed to deal with these security issues in typical IT systems, special precautions must be taken when introducing these same solutions to ICS environments. In some cases, new security solutions are needed that are tailored to the ICS environment.[2]

A number of isolated incidents typified initial concerns. In Australia in 2000 a disgruntled employee accessed the community waste management system and released a large amount of sewage. In 2003 malware penetrated an Ohio-based nuclear power plant disabling a safety monitoring system for nearly 5 hours. The 2010 *Stuxnet* attack exposed vulnerabilities and raised visibility. For the first time specific systems were targeted.

Security challenges now extend from power generation to distribution. The traditional electrical power grid is currently transforming into a ”Smart Grid”, an integrated network that relies on digital and advanced technologies to monitor and manage in real time the transmission and distribution of electricity from generation sources to end users. The advantages are clear. Real-time situational awareness will facilitate operator optimization and may inform consumer behavior. Smart Grids also pose challenges, not least exposure to the threats SCADA systems face. In addition Smart Grid equipment and systems are provided by many industry sectors that historically have not worked together”[3] yet need to be coupled and

[1] Robert O’Harrow Jr. *Cyber search engine Shodan exposes industrial control systems to new risks*, Washington Post Special Report Zero Day 3 June 2012, http://www.washingtonpost.com/investigations/cyber-search-engine-exposes-vulnerabilities/2012/06/03/gJQAIK9KCV_story.html accessed 19 February 2014

[2] Keith Stouffer, Joe Falco and Karen Scarfone. Guide to Industrial Control Systems (ICS) Security, Special Publication 800-82, National Institute of Standards and Technology, June 201, page 3-1 http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf accessed 19 February 2014.

[3] International Energy Agency, “Technology Roadmap: Smart Grids”, 2011, page 31

to share information. "The physical and institutional complexity of electricity systems makes it unlikely that the market alone will implement Smart Grids on the scale that is needed."[4] Public/private collaboration will be needed to define requirements, address concerns and implement solutions. Meanwhile the "smartening" of grids is underway. As a recent threat assessment notes:

> Critical Infrastructure and their main components Industrial Control Systems (ICS) have and are still considered as main potential targets of highly capable threat agent groups, namely terrorists and nation states… Smart Grids are an ideal representation of critical infrastructures: being a very complex system combining both legacy and innovative systems; and playing a key role for energy distribution in the years to come.[5]

It concludes that "the main cause of threat exposure in this area emerges from the technology diversity, component integration, coordination level and cyber security preparedness of the actors in the supply chain" and offers "known incidents in the reporting period show that the energy grid is one of the main targets of cyber-criminals".[6]

This is neither an abstract nor a distant problem. The recent Public Report published by the Canadian Security Intelligence Service (CSIS) noted:

> CSIS is also aware of a wide range of targeting against the private sector in Canada. The main targets are high technology industries, including the telecommunications sector. However, the Service is also aware of attacks against the oil and gas industry and other elements of the natural resource sector, as well as universities involved in research and development.[7]

Both SCADA and Smart Grid infrastructure and infostructure is "owned" and operated by the private sector. However, the "increasing dependence on connectivity for the normal functioning of society makes the protection of connectivity a critical issue for all"[8] and a concern for government. Government has a role to play as a regulatory authority, source of information and intelligence and agent of last resort coordination response measures. The challenge for government is to determine its role, establish partnerships and contribute to the creation of the supporting organization, processes and structures to foster cyber resilience.

1.2 The Centre for Security Science

The Chemical, Biological, Radiological and Nuclear (CBRN) Research and Technology Initiative (CRTI) was launched in May 2002 as the federal science community's response to 911. The intent of the program was to provide science solutions to CBRN terrorist threats. In 2006, following a formal evaluation, the CRTI model was expanded reflecting both the success of the CRTI model and a broadening understanding of security environment. New mission areas – Critical Infrastructure Protection (CIP),

---

[4] Ibid, page 5.
[5] European Union Agency for Network and Information Security, ENISA Threat Landscape 2013, 11 December 2013, page 43. http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
[6] Ibid, page 43-44.
[7] Canadian Security Intelligence Service, Annual Public Report 2011-2013, pp. 19.https://www.csis.gc.ca/pblctns/nnlrprt/2011-2013/rprt2011-2013-eng.asp
[8] World Economic Forum, Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience, June 2012, page 11, http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf

Surveillance, Intelligence & Interdiction (SII) and Emergency Management & Systems Interoperability (EMSI) added included in the Public Security Technical Program (PSTP). As shown (Figure 1), e-Security was distinguished as a cluster and element of CIP. Concurrently the federal government established the Centre for Security Science (CSS) as an arm of Defence Research and Development Canada (DRDC) and a joint endeavor between the Department of National Defence and Public Safety Canada. The new Centre assumed responsibility for overseeing both the CRTI and PSTP. The Canadian Police Research Centre merged with CSS in 2007, bringing police, fire and emergency medical services into the mix. CSS' mission is to strengthen, through investments in science and technology, Canada's ability to prevent, prepare for, respond to, and recover from accidents, natural disasters, or terrorist and criminal acts that impact the safety and security of Canadians.

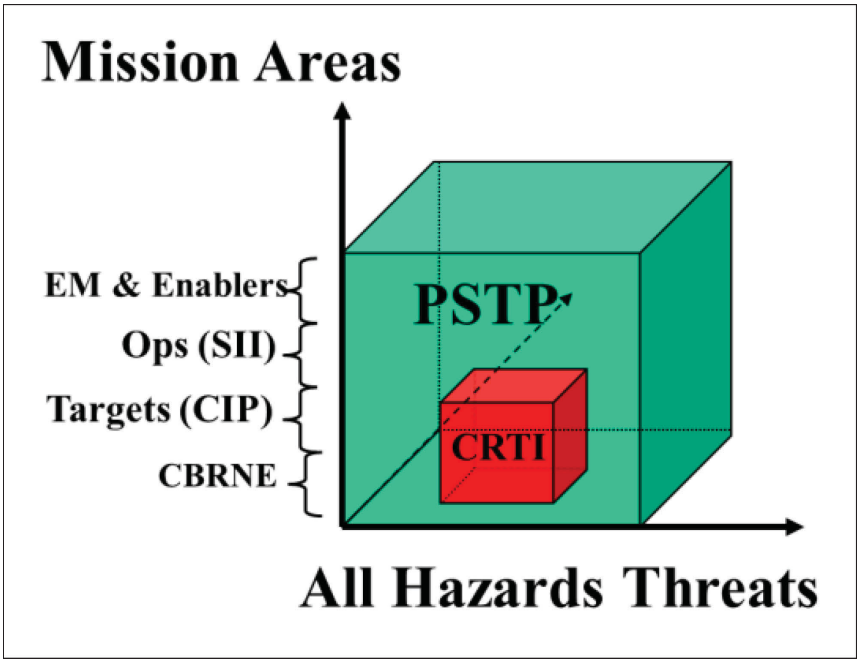


Figure 1 CRTI & PSTP

Table 1: PSTP

Defeat CBRNE Threat	**Critical Infrastructure Protection**
• Defeat Chemical • Defeat Biological: • Defeat Radiological Nuclear • Defeat Explosives: (co-leads)	• Critical Infrastructure Vulnerability, Resiliency & Interdependencies • **e-Security (Cyber)**
Surveillance, Intelligence & Interdiction	Emergency Management & Systems Interoperability
• Biometrics for National Security • First Responder, Policing and Officer Safety • Border and Transportation Security liked to WG • Forensics	• Risk and Vulnerability Assessment • Emergency Management Systems Interoperability • Psycho-Social

Elements of CRTI and PSTP were retained when the program was reviewed and refreshed in 2012 i.e. after a second 5 year term; specifically, emphases on leveraging science and technology and partnerships. The Canadian Safety and Security Program (CSSP) amalgamates and extends prior mandates and provides for greater flexibility in investment distribution and program management. The e-Security program supports implementation of the Government of Canada policies.

1.3 Policy Drivers

It is policy, strategy and plans which drive programs. Public Safety Canada (PSC) recognizes this evolving risk context. The *National Strategy for Critical Infrastructure* published in 2009 provided a definition of critical infrastructure (processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and effective functioning of government), distinguished ten critical infrastructure sectors (energy and utilities, finance, food, transportation, government, information and communication technology, health, water, safety and manufacturing) and described fundamental concepts and principles.[9] Two observations are particularly relevant. The first is that the Strategy proposed to establish networks for each of the critical infrastructure sectors. Their function would be to promote timely information sharing, identify issues and concerns, exploit subject matter expertise (SME) to offer advice and guidance and develop tools and best practices for strengthening sector resilience. The second is to draw attention to the central role IT plays in a number of these sectors, not least energy and utilities. An action plan followed which outlined three key thrusts – partnerships, risk management and information sharing.[10]

[9] Public Safety Canada, National Strategy for Critical Infrastructure, 2009, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-eng.aspx accessed 13 February 14

[10] Public Safety Canada, Action Plan for Critical Infrastructure, 2009 http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr/index-eng.aspx accessed 13 February 14.

CSS's recognition of the increasing importance of e-Security proved timely. *Canada's Cyber Security Strategy* (CSSC) was published in 2010.[11] It acknowledged the increasing dependence on information and networks, discussed threats and societal vulnerabilities, and underscored the importance of cyber security. The CCSS is built on three pillars

- Securing Government systems
- Partnering to secure cyber systems outside the federal Government
- Helping Canadians to be secure online

As an earlier assessment concluded, the challenge is "one of protecting an information-based society as a whole rather than protecting information infrastructures".[12] Progress is being made on three fronts. With established links to industry, academia and allies and a mandate to work across government, CSS is well positioned to contribute to all three thrusts and particularly well positioned to support Pillar 2 and assume an initiation and facilitation role.

1.4 CSS Program Backdrop

The e-Security portfolio has developed in response to policy and organization evolution and maturity. The threat to critical infrastructure and need to establish public partnerships was recognized in policy but more difficult to realize in practice. Government stakeholders focused initially on Pillar 1 and securing government systems. CSS determined that it could exploit and strengthen its links to industry and academia and contribute more to Pillars 2 and 3. The shift from concepts and studies to capabilities and outcomes was equally significant and the detrimental impact of interruptions in service is all perceived to be increasing. Cyber Security management is an attempt to understand, prepare for, and mitigate security events. It is hindered, in part, by gaps in the understanding of how systems are connected, and how those connections result in cascading impacts to other systems. This restricted systemic view and the potential for cascading impact events make planning for security events difficult.

1.3.1 PSTP 02-347 eSec

It has been suggested that "in cyber-space collective responsibility can't be avoided".[13] The origins of the NEITC concept can be traced directly to an early community-led e-Security project. The objective of PSTP 02-347eSec was to define the problem space and establish a baseline understanding of cyber-threat environment affecting SCADA systems with a view to enhancing resiliency by informing research and development programs and fostering a communal exchange of security practices. Complementary objectives included:

- To establish trusted relationships with private sector critical infrastructure SCADA operators;
- To enable the production of research reports on the current cyber-threat environment to SCADA systems;

[11] Public Safety Canada, Canada's Cyber Security Strategy, Government of Canada, 2010 http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx accessed 13 February 14

[12] Angela Gendron and Martin Rudner, Assessing Cyber Threats to Canadian Infrastructure, Occasional Paper Canadian Security Intelligence Service. March 2012, page 23, https://www.csis-scrs.gc.ca/pblctns/cdmctrch/20121001_ccsnlpprs-eng.asp accessed 19 February 2014

[13] Security and Defence Agenda. Cyber-security: The vexed question of global rules, page 23, http://www.mcafee.com/in/resources/reports/rp-sda-cyber-security.pdf accessed 14 February 14

- To contribute to the development of a cyber-threat management system for continued situational awareness; and

- To contribute to the development of best practices for the security of SCADA systems.

Over 65 partners contributed to the report which concluded that:

- The volume of SCADA related research and information was daunting and significant;

- The number of standards, recommended practices, guidance and tools was increasing; and

- Effective exploitation and deployment of security countermeasures was contingent in part on asset owners' technical expertise and awareness.

This initial foray affirmed the requirement for improving and sustaining collaboration i.e. a hub/rally point and centre for fostering the exchanging of SCADA related information.

1.3.2 Document Structure

This document consists of the following sections:

- Section One outlines the project background;

- Section Two describes the NEITC concept and development in detail;

- Section Three discusses complementary initiatives and ongoing projects; and

- Section Four offers a summary and reflections and recommendations on the Way Ahead.

2 National Energy Infrastructure Test Centre

Accumulating risks associated with factors such as increased urbanization, critical infrastructure dependencies and interdependencies, terrorism, climate variability and change, animal and human health diseases and the heightened movement of people and goods around the world have increased the potential for various types of catastrophes. The pace has accelerated, and challenges and focus shifted from abstraction and study to operations and implications. Connectivity and interdependence has increased; cyber security events can readily transcend network and geographic frontiers requiring intelligence sharing across traditional organizational boundaries and challenging Federal/Provincial/Territorial emergency management configurations. Finally the threat axis has mutated. It has moved from merely scanning for and taking advantage of vulnerabilities to more sophisticated reconnaissance and exploitation incorporating targeting and use of advanced persistent threats (APT) and zero-day attacks. What has been described as a "set and forget" approach to resiliency is no longer adequate. Clearly new pro-active concepts and structure are needed in response.

2.1 Concept

The National Energy Infrastructure Test Centre (NEITC) originated as a concept, prompted by the need to inspire and coordinate a response to an increasing threat. It was and is intended to be more instantiation of a capability than simply bricks and mortar and it was recognized from the onset that it would involve the mobilization of expertise, elaboration of protocols for pooling information as well as the creation of shared physical facilities.

Six distinct sub-objectives were identified:

- Hands-on Training;
- Research & Development Initiatives;
- Exercising and testing the deployment of security technologies;
- Development of best practices;
- Conferences and workshops
- Site assessments

2.1.1 Training

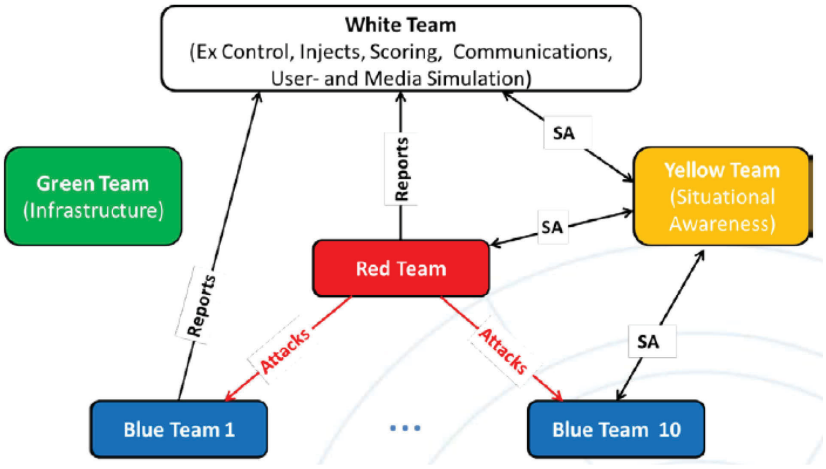
It was envisaged that NEITC Training would provide for a transfer and teaching of expertise and experience and generation and expansion of a knowledgeable workforce equipped to detect and counter ICS/SCADA related cyber-attacks. The NEITC training would address and improve capability, capacity, productivity and performance. It would exploit and complement the core set of skills and foundational content taught at institutes of technology (also known as technical colleges or polytechnics). In addition to basic training, it was recognized that there is a need to confront currency challenges and cater for continuation training, the requirement to maintain, upgrade and update skills throughout working life i.e. fostering and institutionalizing professional development.

It was expected that a range of courses would be required. This might include basic, intermediate and advanced training and shorter introductory/familiarization coursing for executives. Conceptually courses might include both discussion of illustrative use cases and employ scenario based Red, Blue and White team exercises. The military has made good use of this approach. One group of security pros - a Red Team attacks something, and an opposing group - the Blue Team defends it. Originally, the exercises were used by the military to test force-readiness. In traditional warfare, the good guys may intentionally delay capturing a spy so they can learn more about the spy's activities. It works the same way in a cyber-war: a Blue Team can determine whether to block a Red Team probe immediately or attempt to learn more before taking action. The White Team assesses the exercise providing dedicated and objective analysis and directing and informing desired outcomes.[14] This concept has making its way into the corporate world; for example, war gaming the security infrastructure. Every organization, whether part of the government or the private sector, needs "battle-tested" IT personnel in order to detect and defend its networks and information against infiltration and exfiltration. The most effective way to safely simulate this experience is to recreate credible scenarios based on past attacks and known vulnerabilities. Often called cyber war-gaming, these exercises bring IT personnel from different specialties (network, security, virtualization, software, etc.) into color-coded Red, White, and Blue Teams that are assigned specific roles. The Red Team's job is straightforward, to seek and disrupt or destroy. The Blue Team's job is to react and defend. A Red Teamer will use every tool available to compromise a target network and tear down the Blue Team's defenses, with the ultimate goal of taking control of one or more critical systems in order to spy, spoil or sabotage. In today's world of crippling cyber-attacks and dynamic applications, organizations need to know that their networks are secure enough to handle the worst that cyber criminals can throw at them. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are simple to configure, as are Transfer Control Protocol (TCP) SYN flood, half-open attacks, Internet Control Message Protocol (ICMP) volumetric attacks, and others network attacks methods.

---

[14] As suggested Red, Blue and White teams are often used to support military exercises. It is interesting to note that the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) also introduced Green and Yellow teams responsible for Infrastructure and Situational Awareness into the equation in Exercise Locked Shields 2013 conducted 23-26 April 2013. NATO Cooperative Cyber Defence centre of Excellence. Cyber Defence Exercise Locked Shields 2013 After Action Report, Tallinn 2013 http://www.ccdcoe.org/publications/LockedShields13_AAR.pdf accessed 14 February 14.

The following diagram summarizes the exercise construct and team roles:



Typically, setting up such an exercise requires construction of an elaborate infrastructure of servers, network equipment, and security devices, and countless man-hours to configure both the infrastructure and the attack and defense scenarios. A course could be structured to provide Control System engineers with sufficient IT security knowledge to enable them to participate in the exercises. The exercise, in turn, would a vehicle for reinforcing learning. That is, hands-on training would be used to support instruction and allow participants to respond to simulated ICS/SCADA attacks and make mistakes and gain experience and confidence in a "safe" environment. The NEITC training envisaged could have a major impact on establishing Standard Operating Procedures (SOPs) and informing relationships, e.g. determining how IT personnel, control system engineers, law enforcement and intelligence investigators should interact during the course of a significant cyber event. This would contribute directly to ensuring and enhancing resilience of the national, and critically important, Energy and Utilities infrastructure. The observations made during the training lead to the development of improved security measures and incident response plans.

2.1.2 Research and Development

This second sub-objective complements Training and supports Testing. Potentially an NEITC offers a controlled environment for research and development. This could include articulation and elaboration of concepts through modelling and proving of processes to devising and development hardware and software. For example, the forensics research that the RCMP and RTS will perform will help to support how investigators respond to a cyber-incident affecting SCADA networks. The testing of security technologies to identify those that are effective in recovering forensics evidence and safe to operate on a SCADA network is essential. Experimentation and bench testing is a logical extension to gaming.

2.1.3 Testing Technologies

A NEITC also provide a sand-box for trialing and evaluating tools and technologies before they are deployed thereby both familiarizing owners and operators with strengthens and weaknesses and mitigating risk. To realize this intent, the test-bed should be "open" to both technologies and vendors, able to be readily reconfigured as required and, to gain and sustain community acceptance and credibility, committed to objective assessment and capable of balancing discretion and need to share considerations.

2.1.4 Best Practices

Within the control system community, several different standards exist for information technology and industrial control networks. These standards address a number of challenges and controls that are essential to the functionality of these networks. However, there is little supporting material available to address the challenges involved in securing these systems and insufficient effort has been devoted to ensure that existing overlaps or gaps are identified and resolved. Best practices guides address the concern of how to successfully meet compliance and standards objectives without disrupting ongoing process and networks within the control system. Used together with other certification and accreditation activities, guides assist in enabling control system operators and asset owners to meet their regulatory compliance requirements. Regardless of the specific sector, the processes and activities outlined in best practice guides are universal in application to any control system where routable network traffic, traditional network appliances (such as firewalls), and common operating systems are in use.

2.1.5 Conferences and Workshops

The first three sub-objectives relate in large part to a physical test-bed, the next two - Best Practices and Conference and Workshops – relate more to a NEITC's role as a virtual Centre of Excellence. It envisaged the NETIC establishing itself as an information hub capable of supporting knowledge management and overseeing a national network and ICS/SCADA community. This might include the mandate and capability to arrange cyber security related conferences and workshops. These would not need to be hosted at a physical facility NEITC-occupies, although such a site would have an ability to host conference and workshops. Themes would be interest driven and could range from general threat briefs to introductions to specific technology solutions.

2.1.6 Assessments

It is often a challenge to relate general threats to investment in prevention. Workshops focusing on new threats and specific vulnerabilities can serve as an effective prod. No doubt information helps. However, one of the keys to improving resiliency likely lies in localizing and personalizing. This can be done in part through on-site assessments.

While threats encompass a broad spectrum of vectors, most can be broken down into two areas: physical and logical breaches. Physical breaches may include 'vandalism'-type efforts to sabotage operations, or disruption of services due to natural or man-made catastrophes, such as disastrous storms and large-scale accidents. Logical access breaches can include a wide host of threats such as intentional hacking, inappropriate user access, and the introduction of malware (e.g. Trojan horses and Zero-Day Threats). Logical access breaches, due to the burgeoning interdependence of operations and information technology, are the fastest-growing concern. They are often synonymous with the term 'cyber-attack' in the vernacular of the general public. Assets can best be insulated from each of these types of breaches by a multi-layer – known as Defense-In-Depth – approach to managing known risks and preventing introduction of unknown risks to the protected systems. Defense-In-Depth ensures that an organization evaluates both physical and logical security threats, and subsequently establishes multiple layers of protection, making penetration to exploit any given vulnerability much more difficult. The appropriate line of sight for instituting multi-layer defense begins at the enterprise level and establishes a baseline assessment for comparison of security initiatives across the organization over time.

Combating cyber threats is a significant challenge for the multitude of utility companies that are also wrestling with flat security budgets, aging workforces, shifts in security policies, and a shortage of IT staff qualified to address new types of electronic threats. In implementing a cyber-security plan, utility CIO, IT, and network managers must address the dynamic nature of the cyberspace threat environment and comply with a broad range of security and compliance directives. Meeting these objectives effectively and within budget is often a daunting task but the prosperity and competitiveness of utility companies in the 21st Century depends on effective cyber security. Given these hurdles, few organizations have the in-house capability to effectively develop and implement comprehensive cyber security protocols and are looking for help in developing and supporting their utility business models. A NEITC can contribute to bringing lessons learned and best practices home i.e. help to address:

- Pre-audit assessments, and audit preparedness
- Program structure
- Post-audit remediation
- Risk assessment & management (from a cyber-security perspective)

- Strategic & organizational consulting: (drafting roadmaps and strategies to ensure compliance and enhance security)

- Vulnerability & penetration testing

- Training and employee awareness program development & delivery (helping design policies and procedures, curriculum and programs, conducting training & exercises)

- Physical and logical (defense-in-depth) implementation

Assessments can be tailored to cater to organization objectives. For example they could include:

- Program maturity assessments – a review of an individual utility's security posture and a measurement against overall industry position and trending.

- Risk-based assessments – a review of all systems potentially categorized as critical infrastructure to determine appropriate protections, the degree to which those protections have been implemented, and the amount of residual risk associated with unapplied protections

- Vulnerability Assessments – a review of systems deemed to be critical infrastructure assets to delineate potential threats along with the likelihood of those threats occurring and their impact on the specific asset.

2.2 Development

The World Economic Forum has suggested that there are two approaches to developing public-private partnerships. [15] The first is a vertical or sectorial one and the second is a cross-industry one. The first approach had a number of benefits, not least the existence of sectorial associations and better-defined, common interests. It was also clear that a complementary physical facility would provide a rallying point and would allow for a visible demonstration of sectorial buy-in. This facility would have to provide and be seen to provide a secure environment, one in which collective concerns would be addressed and communal good would prevail.

Sector association representatives were approached to contribute SCADA/ICS software and hardware allowing the Test Center to be constructed quickly and equipped with credible and relevant equipment. The underlying vision was to create an entity that would provide leadership, best practices, training, support, research and testing in support of the Energy and Utility Sector. This approach had obvious advantages including entrée, engagement and education. Working with sectorial associations would provide the representatives opportunities to discover, detect, protect; thus to learn, return and share their new found knowledge with their colleagues and counterparts serving as a multiplier and producing a larger impact.

It was apparent was both organizational and physical focus were needed to establish presence and support a NEITC. A governance structure was needed to encourage dialogue and frame direction and infrastructure and infostructure needed to support research and training. It was important that links be established at both board and working levels, and understood that a model of collaborative ownership

[15] World Economic Forum Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience, June 2012, http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf accessed 6 February 2014, page 27

(shared risk and responsibility) would provide the basis to eventual transformation to a self-sustainment. Concurrently computational systems, data storage, large data visualization screen (for group testing and training) and specialized experimental facilities, needed to be assembled and integrated. This was the initial vision – a core group of committed people and a laboratory facility capable of supporting research and training as a start point. The underlying strategy was to start small and build out, and to avoid prematurely prescription i.e. to appreciate from the onset this was a journey not a trip.

2.2.1 Governance

An Energy and Utilities Sector Network (EUSN) was established in October 2008. It is co-chaired by NRCan and serves as a forum for key stakeholders to raise concerns and consider measures to protect national energy infrastructure.[16] The EUSN has 4 working groups:

- Energy and Utilities Sector Roadmap
- Cyber Security
- Research and Professional Training
- Consensus Approach, looking Forward and Societal Values

Obviously all four working groups have a vested interest in the NEITC concept.

An Advisory Committee to the SCADA test-bed was set up to provide oversight, advice and links to the EUSN and broader Energy and Utilities community. Government partners included NRCan, RCMP, CSIS and DRDC.

The importance of leveraging and buttressing communal networks should not be underestimated. The World Economic Forum views cyber resilience as a socio-technical issue.17 It argues that protecting information and communications infrastructure is a vital element of economic security and that trust and security are sources of offers value and competitive advantage. Further it suggests that many non-technical factors are critical enablers. Such factors "include things such as clarity in the legal code, cyber forensic and investigative capabilities, professionals throughout the criminal justice chain who are capability of processing such cases, adherence to international standards, and formal and informal links with the private sector and across borders".18 Cyber resilience can be viewed as both a system of systems and network of networks.

2.2.2 Facilities

Many of the sector operations centres reflect are state of the art and combine data fusion, visualization, analytics (including anomaly detection) and command and control capabilities. NEITC ambitions were more modest and there was no requirement to attempt to replicate one of these.

[16] NRCan's portfolio agencies include the National Energy Board, Canada-Nova Scotia Offshore Petroleum Board, Canadian-Newfoundland & Labrador Offshore Petroleum Board, Atomic Energy of Canada and Canadian Nuclear Safety Commission.

[17] World Economic Forum Risk and Responsibility in a Hyperconnected World, Insight Report, January 2014, page 5.

[18] World Economic Forum Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience, June 2012, page 19.

Figure 2 Operations Centres

The design of the Test Center matured over time. Owners/vendors/operators provided much of the test bed equipment; the remainder and integration were orchestrated by government partners (Vote 5). Figure 3 and Figure 4 illustrate the current floor plan and layout.

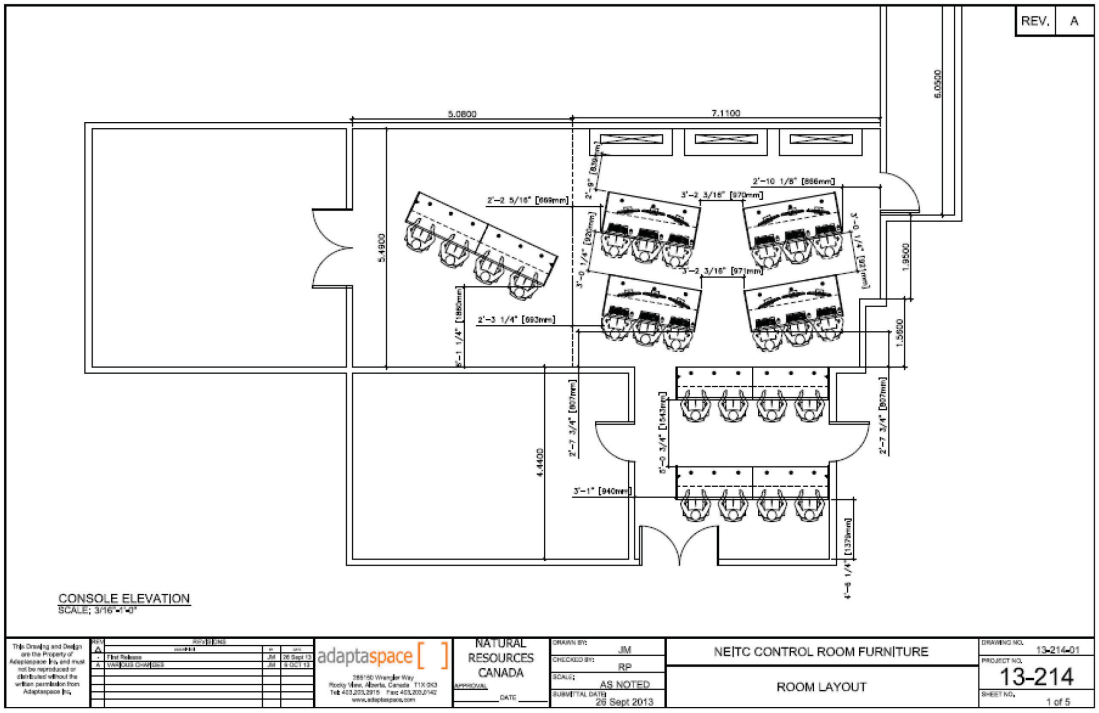


Figure 3 NEITC Floor Plan

Figure 4 NEITC Layout

The NEITC is designed with numerous compartments to provide the capabilities described above. Two major compartments include the testing and simulation area, followed by a number of smaller compartments designed to facilitate the work in the major compartments. The testing and simulation areas are further subdivided including secure data areas. The Data Acquisition (ADA) compartment and the student interaction compartment (Proctor Stations) include within these areas, the hardware and software components encompassing the SCADA systems that monitor, control, safety provisioning and gathering of real-time, high-resolution data for collaboration and visualization. The Server area does the analysis and visualization capabilities beyond what are found in a typical utility operations center. The hardware/ software SCADA systems consist of the following subsystems:

- Remote terminal units (RTUs) which connect to sensors in the process and convert sensor signals to digital data. They have telemetry hardware capable of sending digital data to the supervisory system, as well as receiving digital commands from the supervisory system.
- Programmable logic controller (PLCs) connect to sensors in the process and converting sensor signals to digital data.
- A telemetry system is typically used to connect PLCs and RTUs with control centers, data warehouses, and the enterprise. These include leased telephone lines and WAN circuits. Wireless telemetry media used in SCADA systems include satellite (VSAT), licensed and unlicensed radio, cellular and microwave.
- A data acquisition server that is a software service which uses industrial protocols to connect software services, via telemetry, with field devices such as RTUs and PLCs. It allows clients to access data from these field devices using standard protocols
- The Human Machine Interface (HMI) which provides the interaction within standard protocols found throughout the sector.

The typical manufactures of these systems are equivalent to those that are typically found within the utilities and can be interfaced to the HMIs. Some of the suppliers of these SCADA systems include TCS Technologies, B&D Technologies, Prime Test Automation, Emerson Systems, etc. The Centre does provide the training capability for up to 30 students per session with 3 educators on staff. The educators

are professionals from the industry, academia and government that design and provide various levels of training from basic safety to advanced botnet detection. Within another module of the center, there is capability for advanced cyber security vulnerability, detection, and mitigation analysis.

• Change in Product design and process design can be incorporated easily • More continuity of production in unforeseen conditions like breakdown, shortages, absenteeism	

Fixed location layout

In this type of layout, the product is kept at a fixed position and all other material; components, tools, machines, workers, etc. are brought and arranged around it. Then assembly or fabrication is carried out. The layout of the fixed material location department involves the sequencing and placement of workstations around the material or product. It is used in aircraft assembly, shipbuilding, and most construction projects. A pictorial representation of a fixed location type of layout is given in Figure 3. The advantages and disadvantages are detailed in Table 3.

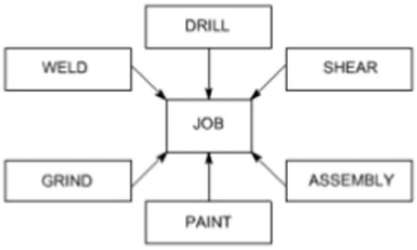


Figure 3: A Pictorial Representation of Fixed Location Type of Layout

Table 3: Advantages And Disadvantages of Fixed Location Type of Layout

ADVANTAGES	DISADVANTAGES
• Material movement is reduced • Promotes pride and quality because an individual can complete the whole job • Highly flexible; can accommodate changes in product design, product mix, and production volume	• May result in increase space and greater work in process • Requires greater skill for personnel • Personnel and equipment movement is increased • Requires close control and coordination in production and

Figure 5Fixed Location Layout – Advantages/Disadvantages

Realization of the vision and instantiation of a NEITC test-bed was realized through a series of discrete projects.

2.2.3 PSTP 03-0431 SCADA Test-bed with Smart Grid

PSTP 03-0431 built upon prior collaboration. Sector and Technical Advisory Committees were consulted and translated broader project goals into more specific objectives. These are described below

Table 2 Goals and Objectives of the SCADA test-bed[19]

Goals	Objectives
1. Enhance the ability of entity system operators and cyber security analysts to detect and respond to a coordinated cyber-attack.	• Use the SCADA Test bed to provide a hands-on simulation of a cybersecurity incident through all phases of detection and response.
2. Provide role-specific training	• Develop a role-specific tiered training program to cover the following functional areas: o Architecture o Operation, maintenance and analysis o Protection, defence and investigation
3. Use of intrusion detection and intrusion prevention tools	• Review the capabilities and limitations of commercially available tools used for intrusion prevention and intrusion detection. o Installation, configuration, and set-up o Best practices for operation and maintenance
4. Perform a forensic analysis	• Secure and retain the evidence needed to analyze the cybersecurity incident without adversely affecting the need to return the SCADA system to operation.
5. Prevention best practices.	• Provide hands-on training to illustrate best practices associated with securing SCADA systems and networks.

[19] National Resources Canada, Energy Infrastructure Security Petroleum Resources Branch & Electricity Resources Branch, SCADA Test-bed with Smart Grid Technologies, PSTO-03-431eSec Project Report, 31 May 2012, page 10.

A laboratory/test centre was constructed within existing NRCan facilities at 615 Booth Street in Ottawa. It was configured to reflect recognized models (e.g. North American Electrical Reliability Cooperation (NERC) Critical Infrastructure Protection (CIP) 005 and International Society of Automation (ISA) S99) and incorporated programmable logic controllers (PLCs), a remote terminal unit and a human machine interface.

Two configurations and two scenarios were generated to support proof-of-concept testing. The first network configuration represented a hydro network (Figure 6) and the second a pipeline model. The first scenario reflected a virus originating from an infected EMail and the second a brute force password attack mounted on a remote site. To distinguish and accommodate Red and Blue teams, two discrete virtual machine images were constructed: one containing attack tools and the second security software.

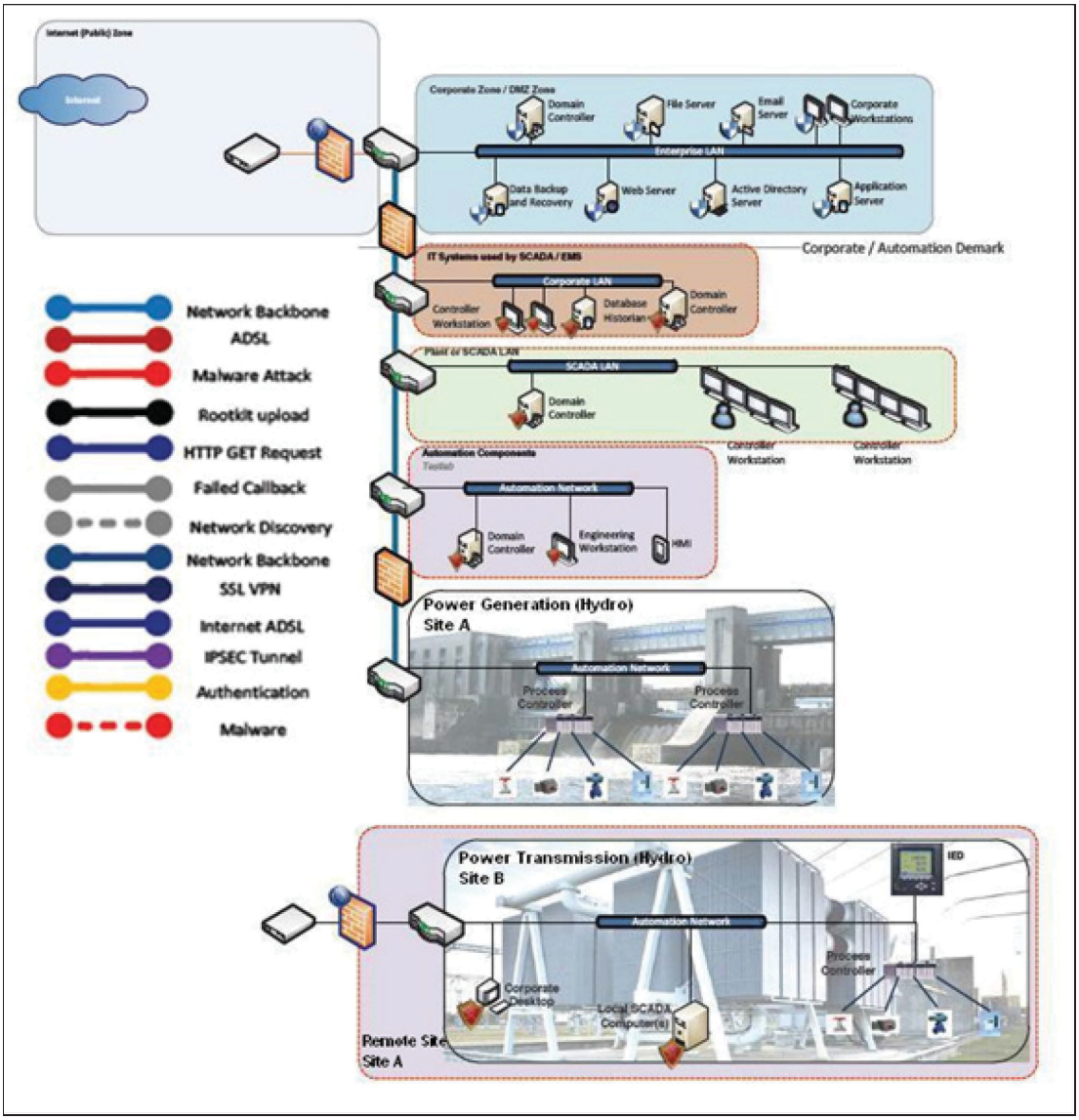


Figure 6 Hydroelectric Generation and Transmission[20]

[20] Ibid., page 19

The proof-of-concept confirmed that the test-bed functioned well and that realistic, scenario-driven exercises could be used to support vulnerability assessments, tool validation and operator training. At the same time, a number of observations followed and a number of challenges were identified:

- The dynamic nature of cyber threats to SCADA systems will necessitate a flexible and adaptable test-bed system;

- Concerns relating to information sharing between public and private sectors will likely necessitate the establishment/enrichment of trusted relationships and may require application of specific, confidential non-disclosure agreements; and,

- The requirement for expanded outreach initiatives with energy sector stakeholders.

2.2.4 CSSP-2012-TI-1034 Integration of the SCADA Testbed and Control, Simulation and Monitoring Room (CSMR) into the National Energy Infrastructure Test Centre (NEITC)

The title describes the project. The objective was to supplement the NEITC test-bed and establish an integrated simulation and control capability. This would better position the NETIC to support research, testing and training.

2.2.5 Initial Operating Capability and Training Session March 2013

A one day course was conducted in March 2013 (Figure 7) and leaders from the oil and gas sector community invited to attend. Participants were exposed to the concept of a NEITC and five scenarios were developed to illustrate security challenges and focus the training. Following the formal session, a questionnaire was used to collect qualitative data. Value statements relating to NEITC objectives were prepared and rated. The feedback indicated that participants judged 'Development of Best Practices' (26.3%) and 'Hands-On Training' (21.1%) offered the greatest return on investment. 'Exercising and Testing the Deployment of Security Technologies' and 'Research & Development Initiatives' were also seen to be significant (15.8% for both objectives); 'Site Assessments' and 'Conferences and Workshops' were each associated with 10.5% of the value statements.

Figure 7 Inaugural Training

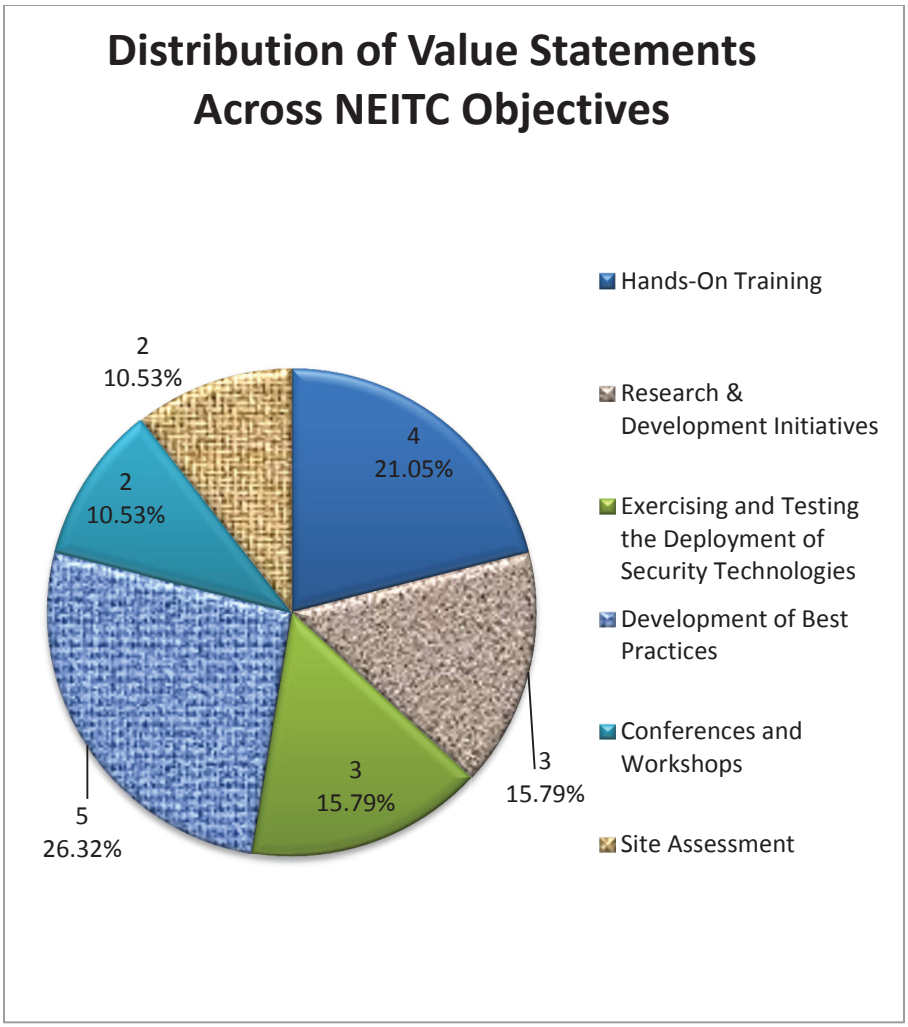


Figure 8 Distribution of Value Statements across NEITC Objectives[21]

These results illustrate clear interest, appetite and initial success of the focused ICS/SCADA training. The "value proposition" was and is acknowledged by the energy & utilities' community. Accordingly a third training session was hosted by the NEITC in November 29 2013 and a fourth is planned for March 2014.

---

[1] [21] Kelly Forbes, National Energy and Infrastructure Test Centre, CAE Technical Note, 4 July 2013, page 8

3 Complementary Initiatives & Ongoing Efforts

3.1 Complementary Initiatives

There are several complementary initiatives which CSS supported.

3.1.1 PSTP 03-423eSec SCADA Network Security in a Test Bed Environment/SCADA Testbed Data Analyzer

In September 2011, work was initiated to create a SCADA network test bed to support Public Safety's Canadian Cyber Incident Response Centre (CCIRC). International test bed initiatives were studied. A model-based approach was adopted and a test bed capable of carrying out evaluation of security devices and supporting forensic investigations developed. It consists of a wall-mounted display panel, industrial control devices in use provided by vendors and a simulator controller, as illustrated below (Figure 9).

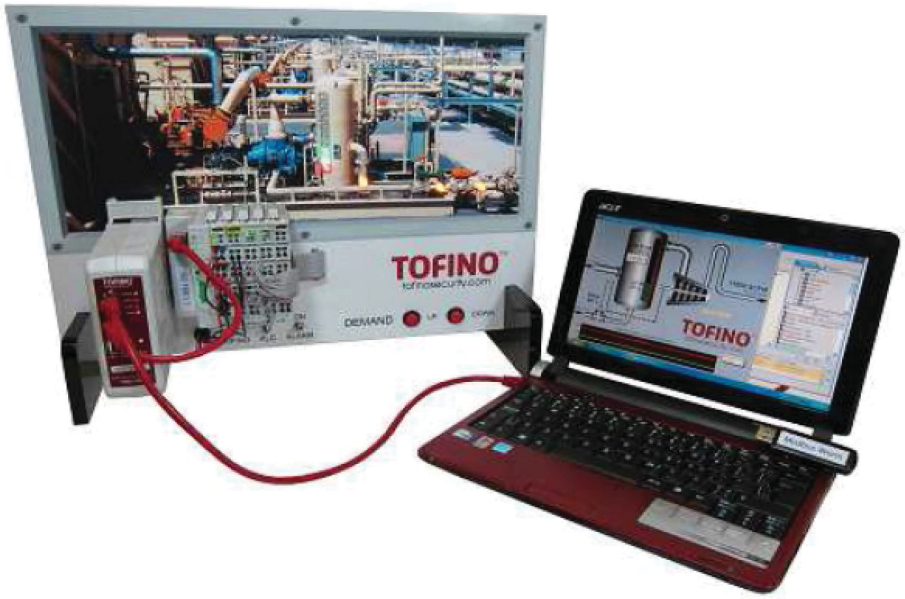


Figure 9 Pipeline Model

Two scenarios/ simulations were developed, one reflecting the oil & gas flows and the other the power generation and (platform software, network and protocol) vulnerability tests conducted. Test tools included Nping, Nmap, SCAPY, Modscan, Achilles and Nessus. The test bed proved appropriate to support CCRICs and a number of vulnerabilities were discovered confirming the requirement for control devices to be upgraded more regularly and more attention to be spent on ICS/SCADA system cyber resilience.

3.2 Ongoing Efforts

There are three projects underway which will progress development, expansion and institutionalization of the NEITC concept.

3.2.1 CSSP-2013-CD-1082 Canadian Power Utility Network Security Smart Grid Workshop

Smart Grid is an upgrade of our existing electrical grids with distributed local intelligence, security, efficiency and upgraded control capabilities. It provides pragmatic solutions on how to transform the existing top down electrical distribution system into a de-centralized grid. Although perhaps years behind when compared with the innovations seen in other technical fields, in terms of size, electric grid systems represent among the largest technical constructions in the world. Smart Grids are central when it comes to addressing environmentally friendly, higher quality, higher efficiency requirements of modern industries and dealing with the rapid increase in energy consumption in emerging countries. Supporting infrastructures are becoming increasingly important as people's expectations and habits change. Statistically, more than half of the world's population lives in cities today. The number of cities with more than 1 million inhabitants has almost doubled from 1990 to 2012 and is still growing. Twenty years ago the average energy consumed in homes was mainly used for "primary needs", such as lighting, heating and cooking; today an increasing amount of energy is consumed by appliances such as multimedia, communication and IT equipment. These differences require a radical rethinking of the way energy is and will be used, and imply a fast transition to Smart cities. This suggests that energy for mobility, lighting, entertainment and "living" will need to be properly and securely managed and accommodate Smart homes which will contribute to minimizing power efficiencies and reducing CO2 emissions. It will also enable renewable energies to be integrated and exploited and facilitate demand/supply balancing. In conclusion, there are many ingredients needed to enable the transition from the current infrastructure to a "smart" infrastructure. These include security, to prevent fraud and malicious attacks; intelligent devices, sensors and MCUs (Multi-Point Control Units), to allow distributed control; efficient power semiconductors, to reduce power losses and offer the reliability needed by a critical service like energy distribution and generation

A one day workshop was held in Vancouver 21 January 2014 as a CSS-sponsored "community development" project. The aim of the workshop was to note trends, share ideas and discuss best practices with a view to gaining a richer understanding of Smart Grid technologies and appreciation of threats and vulnerabilities.

Key note speakers underscored the continuing integration between Information Technology and Operational Technology (OT) and reliance on mainstream networks, platforms, systems and software. In his presentation the Chief Technology Officer of Toffino Security noted the frequency of attacks, citing the fact that globally 9 per day target the energy sector.[22] Breakout groups focused on Issues, Stakeholders, Mitigation Strategies and the Role of the Community and a questionnaire was prepared to capture exit data. The textual analysis of the discussion on priority issues is reproduced below (Figure 10).

[22] Candid Wueest, Targeted Attacks Against the Energy Sector. Semantic, 13 January 2014, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf accessed 17 February 2014

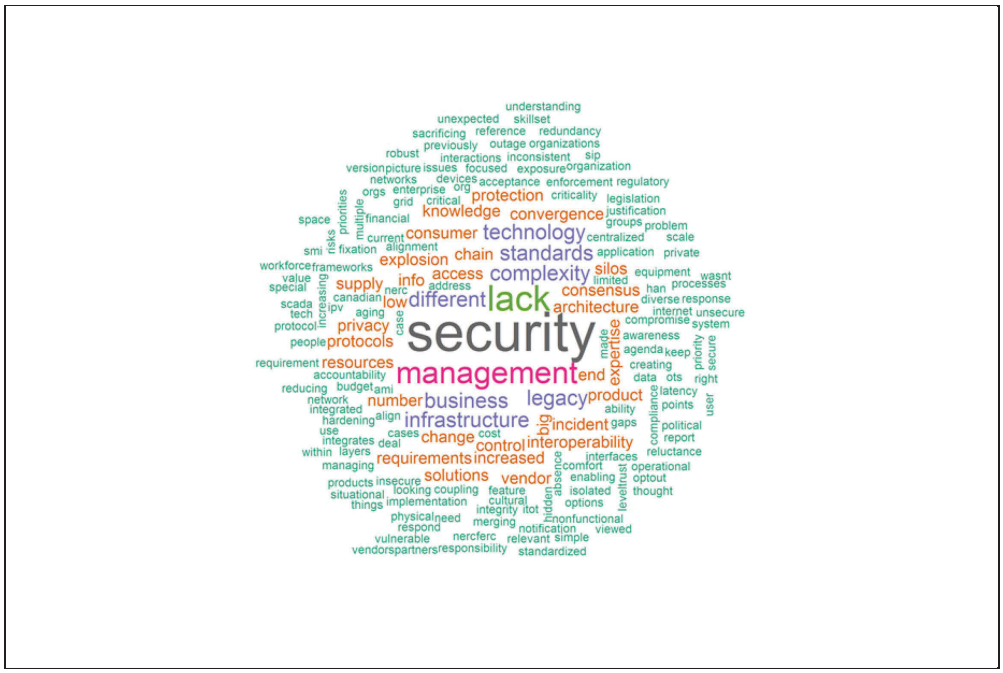


Figure 10 Smart Grid High Priority Issues[23]

Significantly, themes common to those leading to establishment of a NEITC earlier were identified. High priority security concerns reflected the need for more governance, standards and protocols and awareness. Training and compliance were seen to be potential mitigation strategies; finally, participants acknowledged communal responsibilities for providing leadership and sharing knowledge. The "educate, explore, engage, execute"[24] model adopted in pursuing creation of a NEITC appears to offer a sound way forward.

3.2.2 CSSP-2103-TI-1044

This project builds upon prior investment and the inaugural courses held in November 2012 and March 2013. Scenarios will be developed and introductory, intermediate and advanced hands-on training designed and delivered. A course was held in November 2013 and a second is planned for March 2014. In addition NRCan is leading the effort to develop a business plan to consider self-sustainment options i.e. to move from conceptualization to institutionalization.

[23] British Columbia Institute of Technology (BCIT), Group for Advanced Information Technology, Report on Smart Grid Security Workshop, Draft Report Version 1.5, 14 February 2014, page 17

[24] IBM recently suggested this four stage model as an approach to be used in adopting and expanding use of big data. IBM Institute for Business Value, Analytics: The real-world use of big data, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=XB&infotype=PM&appname=GBSE_GB_TI_USEN&htmlfid=GBE03521USEN&attachment=GBE03521USEN.PDF accessed 20 February 2014. In hindsight, it provides an apt description of the approach used to introduce and implement the NEITC concept.

3.2.3 CSSP-2013-TI-1044 Smart Meter Cyber Security Vulnerability Study

The objective of this "targeted investment" project is to explore the security vulnerabilities with Smart Metering Infrastructure (SMI) data communication technologies such as ANSI C12.22. The study will consider not just vulnerabilities in the standard itself, but with various meter vendors' implementation of the standard. It will also explore mitigation approaches and make recommendations for best practices to address these vulnerabilities.

4 Summary and Conclusion

Know your enemy, understand your network, grow your people.[25]

Increasingly Canadian productivity and competitiveness relies on its digital economy. As such, it is a prime target for cybercrime because of its advanced ICT infrastructure, rate of adoption and increasingly internet -mediated and interdependent financial and payments systems and critical infrastructure control systems. While primary responsibility for protecting these systems rests with the owners and operators, government has a crucial role to play providing private sector partners with timely, accurate intelligence risks and threats and overseeing the coordination of responses to large scale incidents. Ensuring the availability, integrity and confidentiality of information is a collective responsibility. *National Strategy for Critical Infrastructure* acknowledges the threat and distinguishes key sectors. *Canada's Cyber Security Strategy* distinguishes Pillars and both documents underscore the importance of public-private partnerships and of collaboration and innovation.

The energy and utilities sector provided an ideal departure point. Canada has a rich endowment of energy resources, which will continue to be important for driving its own economic growth and development, while also being one of its dominant exports. There are also enormous changes taking place in the energy sector around the world, in North America and in Canada. As described in this paper, the introduction and exploitation of modern technologies to improve the efficiencies and effectiveness and reduce cost of energy production and distribution has and will continuing to reshape the landscape. Expanded connectivity will increase interdependencies and introduced new vulnerabilities and concerns. Fortunately the energy and utilities sector has established associations and relationships with government, notably NRCan. These were used to best advantage.

As presently constituted the NETIC offers both value to the community and a portent of what it could contribute. Some of the offerings are tangible, others less so. It began as a concept. It was recognized that a communal response was required and that this would involve creating processes and structure for enhancing information sharing and addressing systemic challenges. Dialogue and investigation identified six distinct roles that a NEITC could play. These ranged from sponsoring research to testing equipment and determining best practices through to hosting workshops and conducting courses to organizing on-site assessments. Every journey begins with a first step, and it was appreciated from the onset that the community was embarking on a journey not a trip.

First steps involved establishing a governance structure promoting public and private participation and collecting and configuring equipment to create a functioning laboratory capable of supporting testing and training. These were significant accomplishments. Inaugural training was conducted and a formal workshop arranged to further "socialize" the concept and solicit feedback. Next steps involve enriching and formalizing coursing, developing site assessments protocols and practices, and investigating options for institutionalization and transition to self-sustainment. Examination should address the adoption and application of Smart Grid which serves a trailing corollary. Smart Grid confronts many challenges that ICS/SCADA owners and operators have met and are facing. In light of this convergence thought should be given to expanding the scope of a NEITC.

This program, implemented as suite of projects, provides a number of lessons. Engagement began with a community-driven threat assessment. This helped established a baseline, a common appreciation of challenges. It addressed the challenges posed what the US Department of Homeland Security recently

[25] Adapted from the adage in a recent White Paper: "know your threat, know your network, know your people".

termed information asymmetries.[26] The post-harmonization CSSP adroitly integrates demand (call for proposal) and supply (targeted investments) driven approaches and also accommodates sponsorship of community development initiatives. "Projectizing" development of the NEITC facilitated management and allowed for review and adjustment. This flexibility ensured that S&T remained in lock-step with ICS/SCADA practitioners.

The notion of designing an environment in which factors can be controlled and experiments conducted is not new. Creation of a sandbox, derived from the field of software programming, reflects an extrapolation of the concept. It appears to be exceptionally well suited to many aspects of cyber security such as ICS/SCADA and Smart Grid where technology is evolving rapidly and the risk to systems and services preclude operational testing. CSS' role would be directed more to facilitating the establishment of the sandbox and empowering communities of practice than to stipulating products. The sandbox concept is now being applied to CSSP-2013-TI-1045 Canadian National Cyber Forensics Capability. A collaborative partnership with the National Cyber Forensics Training Alliance (NCFTA), a Pittsburgh-based not-for-profit, has been set up which will enable Canadian stakeholders, public and private, to establish information sharing protocols and collectively determine the way forward to detect identify, mitigate and neutralize cyber threats. Meanwhile a fledgling NEITC is up, running and evolving. Training is planned for March 2014 and protocols and practices for on-site assessments are being developed on behalf of the energy and utilities sector.

In conclusion, the key to the emerging and documented of the NEITC is clearly the collaborative partnership. Key Federal partners have co-invested to create a "sandbox", an ecosystem capable of supporting research and training and seen to contribute value to SCADA security to owners and operators in the energy and utilities sector.

[26] Department of Homeland Security, Integrated Task Force. Executive Order 13636: Improving Critical Infrastructure Cybersecurity , 12 June 2013, page 26 http://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf

Bibiliography

[1] Aillerie, Said Kayal, Jean-Pierre Mennella, Raj Samani, Sylvain Sauty nd Laurent Schmitt. Smart Grid Cyber Security, Intel White Paper http://www.mcafee.com/ca/resources/white-papers/wp-smart-grid-cyber-security.pdf accessed 19 Februaryruary 2014.

[2] British Columbia Institute of Technology (BCIT), Group for Advanced Information Technology, Report on Smart Grid Security Workshop, Draft Report Version 1.5, 14 Februaryruary 2014

[3] Canadian Security Intelligence Service, Annual Public Report 2011-2013. https://www.csis.gc.ca/pblctns/nnlrprt/2011-2013/rprt2011-2013-eng.asp accessed 6 Februaryruary 2014

[4] Department of Homeland Security, Integrated Task Force. Executive Order 13636: Improving Critical Infrastructure Cybersecurity , 12 June 2013 http://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf accessed 14 February 14

[5] European Union Agency for Network and Information Security, ENISA Threat Landscape 2013, 11 December 2013, http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats

[6] Fabro, Mark. Study on Cyber Security and Threat Evaluation in SCADA Systems, DRDC CSS CR 2012-006

[7] Forbes, Kelly. National Energy and Infrastructure Test Centre, CAE Technical Note, 4 July 2013

[8] Gendron, Angela and Martin Rudner, Assessing Cyber Threats to Canadian Infrastructure, Occasional Paper Canadian Security Intelligence Service. March 2012, page 23, https://www.csis-scrs.gc.ca/pblctns/cdmctrch/20121001_ccsnlpprs-eng.asp accessed 19 Februaryruary 2014

[9] Howes, Rodney and Andrew Vallerand. SCADA, Analysis of the Operational Value of the National Energy Infrastructure Test Centre, DRDC CSS DSTPS 3780-1

[10] IBM Institute for Business Value, Analytics: The real-world use of big data, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=XB&infotype=PM&appname=GBSE_GB_TI_USEN&htmlfid=GBE03521USEN&attachment=GBE03521USEN.PDF accessed 20 February 2014

[11] International Energy Agency, "Technology Roadmap: Smart Grids", 2011, http://www.iea.org/publications/freepublications/publication/name,3972,en.html

[12] Kwamena, Felix. SCADA Test-Bed with Smart Grid Technologies, PSTP 03-431eSec Project Report, DRDC CSS, 31 May 2012

[13] Kwamena Felix and Andrew Vallerand. National Energy and Infrastructure Test Centre (NEITC) Way to Sustainability, Discussion Paper, DRDC CSS TN 2013-032, 2013

[14] Lemay, Antione, Jose Fernandez and Scott Knight. An isolated virtual cluster for SCADA betwork security research, Proceedings of the 1st Internationals Symposium for ICS and SCADA Cyber security Research, 2013

[15] Robert O'Harrow Jr. *Cyber search engine Shodan exposes industrial control systems to new risks*, Washington Post Special Report Zero Day 3 June 2012, http://www.washingtonpost.com/investigations/cyber-search-engine-exposes-vulnerabilities/2012/06/03/gJQAIK9KCV_story.html accessed 19 February 2014

[16] NATO Cooperative Cyber Defence centre of Excellence. Cyber Defence Exercise Locked Shields 2013 After Action Report,, Tallinn 2013 http://www.ccdcoe.org/publications/LockedShields13_AAR.pdf accessed 14 February 14

[17] Stouffer, Keith, Joe Falco and Karen Scarfone. Guide to Industrial Security (ICS) Security, National Institute of Standards and Techn9ology, US Department of Commerce, Special Publication 800-82 June 2011, http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

[18] Public Safety Canada, National Strategy for Critical Infrastructure, Government of Canada, 2009 http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-eng.aspx

[19] Public Safety Canada, Action Plan for Critical Infrastructure, Government of Canada, 2009 http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr/index-eng.aspx

[20] Public Safety Canada, Canada's Cyber Security Strategy, Government of Canada, 2010 http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx

[21] Public Safety Canada, Action Plan 2010-2015 for Canada's Cyber Security Strategy, Government of Canada, 2013 http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-eng.aspx

[22] Security and Defence Agenda. Cyber-security: The vexed question of global rules http://www.mcafee.com/in/resources/reports/rp-sda-cyber-security.pdf accessed 14 February 14

[23] Solana Networks, SCADA Network Security in a Test Bed Environment, 29 March 2012

[24] Stouffer, Keith, Joe Falco and Karen Scarfone. Guide to Industrial Control Systems (ICS) Security, Special Publication 800-82, National Institute of Standards and Technology, June 2011, http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf accessed 19 February 2014.

[25] Tsang, Rose. Cyberthreats, Vulnerabilities and Attacks on SCADA Networks, University of California at Berkeley, 2010, http://hope.dreamhosters.com/iths/Tsang_SCADA%20Attacks.pdf accessed 19 February 2014.

[26] World Economic Forum, Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience, June 2012, http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf accessed 6 February 2014

[27] World Economic Forum Risk and Responsibility in a Hyperconnected World: Insight Report, January 2014 http://www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf accessed 19 February 2014

[28] Wuesst, Targeted Attacks Against the Energy Sector. Semantic, 13 January 2014, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf accessed 17 February 2014

[29] Zhu, Bonnie, Anthony Joseph and Shankar Sastry. A Taxonomy of Cyber Attacks on SCADA Systems, Department of Electrical Engineering and Computer Sciences, University of California at Berkeley, 2011, http://bnrg.cs.berkeley.edu/~adj/publications/paper-files/ZhuJosephSastry_SCADA_Attack_Taxonomy_FinalV.pdf accessed 19 February 2014

List of symbols/abbreviations/acronyms/initialisms

ADM	Assistant Deputy Minister
APT	Advanced Persistent Threats
CBRNE	Chemical, Biological, Radiological, Nuclear, Explosive
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CONOPs	Concept of Operations
CRTI	CBRNE Technical
CSEC	Communications Security Establishment Canada
CSIS	Canadian Security Intelligence Service
CSS	Centre for Security Science
CSSP	Canadian Safety and Security Program
DG	Director General
DOS	Denial of Service
DDOS	Distributed Denial of Service
DRDC	Defence Research and Development Canada
ICS	Industrial Control Systems
ISA	International Society of Automation
NEITC	National Energy Infrastructure Test Centre
NERC	North American Electrical Reliability Society

NIST	National Institute of Standards and Technology
NRCan	Natural Resources Canada
PLC	Programmable Logic Controllers
PS	Public Safety Canada
PWGSC	Public Works and Government Services Canada
RCMP	Royal Canadian Mounted Police
R&D	Research & Development
SA	Situational Awareness
SCADA	Supervisory Control and Data Acquisition
SME	Subject Matter Expert
SOP	Standard Operating Procedures
SSC	Shared Services Canada
TBS	Treasury Board Secretariat

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

DRDC Centre for Security Science
222 Nepean Street
Ottawa, ON
K1A 0K2

2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

UNCLASSIFIED
(NON-CONTROLLED GOODS)
DMC A
REVIEW: GCEC April 2011

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

National Energy Infrastructure Test Centre (NEITC) : Concept and Development of an Entity to Assist in Cyber Protection of Industrial Control Systems within the Energy and Utilities Sector in Canada

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

Howes R.; Hales D.; Vallerand A.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
March 2014	45	29

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Technical Memorandum

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
CSSP-2012-Ti-1034; CSSP-2013-CD-1082; CSSP-2013-TI-1044	

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC CSS TM 2013-055	

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)
Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

Awareness of the vulnerability of SCADA and ICS networks increased dramatically following exposure of the 2010 Stuxnet virus which targeted Iran's nuclear facilities. This was the first publicly known attack on a programmable logic controller and highlighted the need for better testing and monitoring capabilities and more effective collaboration and training. Risk precludes using "live" systems; hence, an independent, complementary capability was needed. A requirement to integrate digital and physical components of SCADA and ICS systems and an opportunity to exploit emulation and simulation were identified. The concept of a "sandbox" used by software programmers to run untested code or untrusted programs in isolation was adopted. Several Federal partners collaborated to create an ICS test and training centre. This report summarizes key elements of the concept and development of the nascent National Energy Infrastructure Test Center (NEITC)

La découverte en 2010 du virus Stuxnet, qui ciblait des installations nucléaires en Iran, a révélé les graves lacunes que présentent les réseaux de systèmes de contrôle et d'acquisition de données (SCADA) et les réseaux de systèmes de contrôle de processus (SCI). Première attaque divulguée au public, elle visait un contrôleur logique programmable et a mis en évidence la nécessité de disposer de meilleures capacités d'essai et de surveillance, ainsi que d'une collaboration et d'une formation plus efficaces pour contrer un tel problème. Comme l'utilisation de systèmes opérationnels présente trop de risques, il fallait donc recourir à une capacité complémentaire et indépendante. On a constaté que les composantes numériques et physiques des systèmes SCADA et SCI devaient être intégrées, et qu'on avait là l'occasion de tirer parti des technologies d'émulation et de simulation. On a alors adopté le principe du « bac de sable » que les programmeurs appliquent en milieu isolé lorsqu'ils exécutent du code ou des programmes non testés. Plusieurs partenaires fédéraux ont participé à la mise sur pied d'un centre d'essai et de formation sur les SCI. Le présent rapport résume les éléments clés du concept et de l'établissement du nouveau Centre national d'essai de l'infrastructure énergétique (CNEIE).

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

SCADA; Cyber Security; National Energy Infrastructure Test Center (NEITC); Testing and Training