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

3780-1 (DSTPS) DRDC CSS LR 2013-048

14 December 2013

LETTER REPORT: ANALYSIS OF THE OPERATIONAL VALUE OF THE NATIONAL ENERGY INFRASTRUCTURE TEST CENTER (NEITC)

BACKGROUND

A National Energy Infrastructure Test Centre (NEITC) was established recently in response to emergent threats to Canada's critical infrastructure (CI)[1]. Supervisory Control and Data Acquisition (SCADA) systems have a broad range of commercial uses and are used widely in the Energy and Utilities Sector. The employment of the *Stuxnet* worm in 2010 highlighted vulnerabilities and illustrated how SCADA systems could be 'hacked' and physical equipment controlled remotely. The establishment of a test bed followed by addition of complementary simulation capabilities was supported by a project team consisting of NRCan, DRDC, RCMP, CSIS and PS Can. Inaugural training was conducted and a plan for transition to self-sustainment is currently under development[2].

Although initiated by government, from inception, it was appreciated that to realize its potential, the NEITC must operate as a public private partnership. In March 2013, members of the oil and gas industrial community, leaders in their respective domains, were invited to and participated in a **training** workshop inside NEITC. Comments were solicited and feedback in the form of formal letters received from approximately 33.33% of the participants. In addition to recording the experience, SCADA-related challenges were identified and the value NEITC could add and the role the NEITC might play were highlighted.

Prior to the inception of the NEITC, an analysis was put in place to determine what was S&T capabilities were needed to assist securing Pillar 2 of the National Security Strategy which encompassed the Energy producing and distribution sector of the Canadian Economy. To this end, a number of studies and polls were commissioned to help decisions makers comprehend the scope of the problem. From these studies, it became evident that the problem space was complicated and would require measures not normally used, due to the multi facets and political issues facing the Energy sector. It became clear that the primary need was to create an environment that could channel whole of federal government/national involvement. CSS (Centre for Security Sciences) was uniquely positioned as it plays its role in whole of government outcomes. A decision was made to seek out which Federal Department would be best suited to host this capability. Natural Resources Canada became that entity. Next, an internal champion was needed and chosen, followed by building the vision and ultimately the Center with the Partners. Initial concepts were put in place. A team was assembled from government, academia and industry to refine them. The design phase and build phase followed. The required basic hardware and software components were procured and assembled to build out the NEITC. Concurrently studies were commissioned to determine what precise capabilities the NEITC would offer. It became clear that the Energy and Utilities Sector was asking for S&T efforts that would benefit them while we needed to meet our objectives namely that government was mandated to helping secure Pillar 2 of the NCSS.

Ultimately the NEITC Team focussed on six objectives: 1) Hands-on Security Training, 2) Exercising and testing the deployment of Security Technology, 3) Research and Development Initiatives, 4) Development of Best Practices, Site Assessments, 5) Security Workshops and 6) Security Conferences.

[1] Kwamena, F. SCADA Test Bed and Smart Grid (PSTP-3-0431eSec). NRCan Report 2013-2, DRDC CSS, 2013.
[2] Kwamena, F. & Vallerand, A. National energy and infrastructure test centre (NEITC) way ahead to self-sustainability: A discussion paper. 17 May 2013. DRDC CSS TN 2013-032, 2013.

The NEITC as a "sandbox" became operational in March 2013 with the first training course delivered at that time. This training took place with the available representatives of the Energy and Utilities Sector and they underwent training with 5 different ICS/SCADA threat scenarios, using their own systems on site at NEITC. Following this training, analysis was done on the effectiveness provided by the Center. Post-workshop feedback was received from representatives of the many organizations and associations. Responses were evaluated by the study team[3] and multiple data points extracted from each source. The feedback was characterized in terms of:

- *Value statements* that related to the information shared and training obtained at the March 2013 workshop. These value statements were categorized using the six NEITC objectives (see above). This approach ensured that a clear association could be made between the value statements and their relevance to the NEITC mandate;
- *Challenge statements* that are presently faced by the ICS (Industrial Control Sector) community; and
- *Future requirements statements* that must be addressed by this sector.

VALUE-ADDED OF NEITC

Value Statements. A total of nineteen value statements were identified in the data analysis. Each of these value statements was relevant to at least one of the six NEITC objectives. Further analysis of the categorized **value statements** revealed most of the value identified in the post-workshop feedback was associated with the '**Development of Best Practices'** (26%) and **Hands-On Training** (21%). To a slightly lesser extent, the post-workshop feedback identified value that was associated equally with '**Exercising and Testing the Deployment of Security Technologies'** and '**Research & Development Initiatives'** (16% for both objectives). Finally, the analysis revealed that '**Site Assessments'** and '**Conferences and Workshops'** were each associated with 10.5% of the value statements.

Challenge Statements. An analysis of the post-workshop feedback also identified challenges facing by the SCADA community. The two primary themes associated with these challenge statements relate to: 1) The requirement for Collaboration and Awareness; and 2) Increasing and Uncertain Cyber Threats.

Future Requirements Statements. An analysis of the post-workshop feedback identified issues relating to the Way Ahead that need to be addressed by the SCADA community. Statements regarding the future fell into two classes. The following primary themes being: 1) NEITC's role in enhancing security; and 2) Funding commitment.

In many ways, all the documented testing and the formal feedback after an ICS/SCADA training with 5 different Scada threat scenarios is serving as an additional measure of verification and validation as well as a measure of the value derived by the Sector partners from using the NEITC. There is general agreement in daily newspapers that threats to ICS/SCADA systems will persist, will grow and evolve while posing a greater risk to Critical Infrastructure owners. The NEITC has demonstrated potential to serve as a rallying point for the SCADA community: a) for offering a venue for testing equipment and uncovering vulnerabilities, b) for facilitating the exchange of threat information and best practices, c) for simulating incidents and d) for providing hands-on training thereby augmenting the national pool of expertise and ultimately starting to contribute to enhanced CI resiliency.

In addition to demonstrating and documenting value-added, the post-workshop findings will shape the way forward. It is noteworthy that the value of the *'Hands-On Training'* and *'Development of Best Practices'* were highlighted by the partners as higher priority elements. Follow-on co-investment by the broader community should provide for further development of scenarios and refinement of introductory, intermediate and advanced training for the partners. It should also provide for collaboration with industry, investigation of governance options and joint development of a business plan for transition to self-sustainment addressing "future statements'. A separate thrust, albeit part of the future efforts, should also investigate development of a 'site assessment' methodology.

In conclusion, this report demonstrates that the NEITC provides value to the Energy and Utility Sector partners. The workshop at NEITC also provided an opportunity to inform and engage the Energy and Utilities Sector, and build consensus within the Community. The findings underscored the importance the SCADA community attaches to the NEITC initiative and the findings are also being used to inform co-investment planning. Not least, the feedback

[3] Forbes, K. NEITC Technical Note. CAE TN 5513-002-02; DRDC Contractor Report, 4 July 2013.

establishes that the joint contributions that have been made by NR CAN, DRDC, RCMP, PS CAN and CSIS in support of the ICS/SCADA community of the Sector are focusing and enriching efforts to address existing and emergent cyber threats as well as to enhance critical infrastructure protection and ultimately, resilience.

Mr. Rod HOWES
Author

Original Signed By

Reviewed by:

Dr. A.L Vallerand
Director, Directorate S&T Public Security
DRDC CSS

Original Signed By

Approved for release by:

Dr. A.L. Vallerand
Document Review Panel Chair
DRDC CSS

Original Signed By

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