



Cyber Safe

Global cyber security experts meet to discuss a coordinated approach on enhanced cyber safety in nuclear power plants

An international contingent of cyber security experts gathered at the CANDU Owners Group (COG) offices and at the Bruce Power nuclear plant, March 19-23, to share knowledge and collaborate on standards and processes to ensure cyber safety and security at nuclear plants worldwide.

The event, co-ordinated by the International Atomic Energy Agency (IAEA) and Bruce Power, was held, in part, to review cyber security initiatives undertaken through the IAEA by the Canadian utilities, Canadian Nuclear Laboratories, the Canadian Nuclear Safety Commission and Global Affairs Canada. It is the second meeting for research coordination on enhancing security incidence response and planning at nuclear facilities. Detailed discussions focus on research activities of each participating institution and the possible harmonization of their approaches to computer security.

“Dealing with cyber threats in isolation is not enough,” said Sarah Shortreed, Bruce Power’s Chief Information Officer. “It requires a strategy and a long-term investment in our capabilities and that’s why the IAEA Coordinated Research Project is so important. Some of the best minds in the industry have come together with a common goal to protect and enhance computer security at nuclear facilities. Through their collective experience and ingenuity we will continue to predict, detect and defeat cyber threats, while using cyberspace to further the interests of the worldwide nuclear industry.”

Cyber security measures in nuclear plants include processes, procedures and technical measures. Combined, these steps can be effective in combatting cyber threats in nuclear plants of all ages and technology generations, says Fred Dermakar, COG President and CEO.

“The information sharing taking place will enhance the knowledge and awareness of all gathered, and by extension, their organizations and our industry,” he says.

“Collaboration is one of the best ways to mitigate the time and money constraints on all of our organizations in order to continue the important work being done, globally on this issue. We’re all in this together.”

Universities and research institutes from Brazil, Austria, Germany, Hungary, Korea, China and the United States presented at the conference.

Focus for the week includes operator support for computer security incident recognition and response, analysis and technology response support, computer security information exchange and cyber crime investigation.

The meeting also showcased the constructed hardware-in-the-loop test beds, plant simulation models and IAEA yearly progress reports.

Safe and Secure

Canadian nuclear plants are prepared for cyber security

Like other countries worldwide, the Canadian nuclear industry has a number of initiatives on cyber security including:

- A COG peer group to share best practices, operating experience and to develop a common approach to meeting the requirements of CSA N290.7, which is a standard for security implementation at Canadian nuclear power plants;
- The Canadian Nuclear Laboratory (CNL) has set up an R&D facility in Fredericton devoted to cyber security; and,
- Canadian utilities, CNL and the Canadian Nuclear Safety Commission are viewed as world leaders in this area through their extensive contribution towards the development of IAEA Cyber Security guidance documents.



An international contingent of cyber security experts met in Toronto and visited Bruce Power, March 19-23, to share knowledge and collaborate on standards and processes to ensure cyber safety and security at nuclear plants worldwide.