Contribution ID: **94** Type: **Interactive Content Presentation**

An Effect-Centric Approach to Assessing and Comparing Cybersecurity Risks against Digital Systems at Nuclear Facilities

Cyber threats are increasingly one of the major threats facing all countries. The high-profile "ransom-ware" attacks by WANNACRY in May 2017 and the TRITON attack against the safety system at an industrial complex in the Middle East in August 2017, and against a second victim recently, served as reminders that cyber risks are real and increasing. In nuclear facilities including nuclear power plants (NPPs), a cyber attack could knock out digital control systems vital to ensuring the security of plants and materials, to an extent causing physical damages or losing human lives. While many assume that critical infrastructure, including nuclear facilities are "air gapped"and not connected to the Internet, in practice the gap can often be compromised as shown in the STUXNET attack against a uranium enrichment facility.

Faced with this rapidly growing cyber threats, the Center for International & Security Studies at Maryland (CISSM) has developed an "Effect-Centric Approach"to assessing and comparing the cyber-security risks . The approach classifies cyber events to be exploitative or disruptive depending on whether the attack motive is to steal company information to the extent of holding them for ransom, or to interfere with operational functions to the extent of causing physical damages. By evaluating the severities of various cyber events, either within the same attack vector or across different scenarios, the Cyber Exploitation Index (CEI) or the Cyber Disruptive Index (CDI) can be devised, and they can be used by organizations in the public or private sector for assessing and comparing cyber-security risks.

In this paper, we apply the CISSM approach to assess and compare the cyber-security risks for NPPs. The assessment would focus on the attack vectors (scenarios) against the NPP's digital instrumentation & control system (e.g., the programmable logic controllers and the Supervisory Control and Data Acquisition, etc.) for both safety and non-safety systems; and follow the scenario progresses to their conclusions. Based on the severity of the end-results (e.g., loss of information, ransom payment, damaged equipment, or devastating on-site or off-site radiological releases, etc.), a CEI or a CDI can be devised for these scenarios. The aim is to provide insight for Information-Technology experts, Operational-Technology staff, supply chain vendors, plant managers, organizational leaders, and policy makers for effective communication and threat identification that differentiate the threats from a private problem to a genuine public concern.

State

United States

Gender

Male

Author: Dr CHOI, Jor-Shan (Lawrence Livermore National Laboratory (retired))

Co-authors: Prof. GALLAGHER, Nancy (University of Maryland); Prof. HARRY, Charles (University of Maryland)

Presenter: Dr CHOI, Jor-Shan (Lawrence Livermore National Laboratory (retired))

Track Classification: CC: Information and computer security considerations for nuclear security