Contribution ID: **600** Type: **Paper**

Digital Hazards Identification: A New Approach to Cyber Security for Nuclear Facilities

Monday 10 February 2020 11:45 (15 minutes)

The increasing use of digital instrumentation and control (DI&C) systems in nuclear power plants (NPP) presents new challenges to traditional security and protection measures. The current focus of cyber security-related research on protecting sensitive information or privileged networks from state-of-the-art "hacker" attacks struggles to adequately address protection needs for digital controls over physical processes. Thus, there is a need for cyber security research to move beyond an "anti-hacker"approach and more systematically identify and describe potential hazards that can be experienced in physical space but initiated (or implemented) in digital space. As is a common struggle across all cyber security efforts, the large number of potential failure modes from DI&C systems challenge the efficacy of deterministic approaches to identify critical digital assets or probabilistic risk assessments (PRA)-based analysis. This suggests that a risk-informed approach is necessary to properly assess the importance of DI&C systems to the criteria outlined in international cyber security best practices and better protect nuclear fuel cycles facilities (and activities) as pieces of critical global infrastructure.

Research funded by the Electric Power Research Institute (EPRI) in the U.S.—in collaboration with the Complex Hazards Analysis for Risk Management (CHARM) Team at Sandia National Laboratories—developed a response founded on key systems engineering concepts as "holistic"system characterization, describing new interactions enabled by DI&C, and illustrating interdependencies between DI&C and non-DI&C elements. Using these concepts, the CHARM team evaluated the appropriateness and adequacy of both traditional (e.g., Fault Tree Analysis, FTA) and novel (e.g., Systems-Theoretic Process Analysis, STPA) hazards analysis techniques for addressing these cyber security challenges. The CHARM team concluded that combining STPA and FTA leverages the benefits and overcomes the shortcomings of the individual methodologies to meet the criteria for risk-informed cyber security methodology—resulting in the Hazards and Consequence Analysis of Digital Systems (HAZCADS) technique. HAZCADS merges the system-theoretic principles of STPA with the probabilistic elements of FTA to efficiently and methodically identify, categorize, and assess hazards that can emerge from digital systems in NFC activities.

HAZCADS better incorporates both the direct and indirect roles of digital components in potential failure pathways and expand upon traditional cyber security approaches by incorporating: (1) the uniqueness and complexity of DI&C components; and (2) newly identified digital failure modes, including those from component interactions that still result with no component failure occurring. This paper will briefly summarize the core tenets of both FTA and STPA, provide a detailed description of how to develop SIFTs, and introduce the overall HAZCADS methodology. Next, a review of several examples of applying HAZCADS will be provided, including a comparison of lessons learned. Finally, this paper discuss several key implications for this new cyber security approach, including more effective application of limited cyber security resources on more vulnerable areas and higher fidelity (and flexible) digital hazard identification approach for NFC activities consistent with international best practices.

SAND2019-6257 A. Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525.

Gender

State

United States

Authors: Mr CLARK, Andrew (Sandia National Laboratories); WILLIAMS, Adam (Sandia National Laborato-

ries)

Presenter: Mr CLARK, Andrew (Sandia National Laboratories)

Session Classification: Identification, Classification, and Protection of Digital Assets in a Nuclear Security Regime

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