Contribution ID: **37** Type: **Paper**

Integrated Safety and Cyber Security Analysis for Building Sustainable Cyber Physical System at Nuclear Power Plants: A Systems Theory Approach

Nuclear power plants (NPP) install digital instrumentation and control (I&C) systems and physical protection systems (PPS) for its safe and precise operation using software-intensive systems and interconnected digital components respectively. The both of these software-intensive digital I&C systems and interconnected systems of PPS interface safety and security systems creating new cyber security threats that can lead to undesirable safety accidents in NPPs. Furthermore, the recent trend of attacks to nuclear installations may take place blended in nature that is cyber and physical attacks happening alongside. Consequently, these system designers encounter difficulties to incorporate these newly issued cyber security requirements in the additional design features of their safety systems. Therefore, integrated safety and cyber security analysis is indispensible part for building a sustainable cyber physical system in the NPPs. Despite the potential of integrating safety and cyber security analysis, NPPs addresses separately when they should not be. Drawing upon these limitations, this paper develops an integrated approach of safety and cyber security analysis at nuclear power plants based on systems theory. A system theory signifies the nature of a complex systems and represents a framework of investigation that later appropriated as Systems-Theoretic Processes Analysis (STPA). STPA is used as a unique safety analysis approach used on a large variety of systems today, including nuclear power plants (Young and Leveson, 2014). In the same way, extended STPA can provide a powerful foundation for cyber security analysis (Young and Leveson, 2014). In this study, we propose an integrated safety and cyber security analysis by combing STPA-Safety and STPA-Security methodology for building sustainable cyber physical system at NPPs. The proposed integrated STPA-SafeSec methodology provides a comprehensive analysis of safety and cyber security. The application of this novel STPA-SafeSec methodology is illustrated using a case study of a risk scenario in a nuclear facility.

NPPs critical digital assents of I&C systems are highly software-intensive which require strong assurance for safety and reliability. These digital I&C systems interface safety and security systems as it collect signals from sensors measuring plant parameters, integrates and evaluates sensor information, monitors plant performance, and generates signals to control plant devices using digital computers, communication system and network technologies. In the same way, a range of common software components, network management tools, operating systems of cameras, access control are gradually being integrated into the PPS infrastructures that support safety-critical system as well. The increasing use of these common components creates concerns that bugs might affect multiple systems across many different safety related components raising significant security concerns at NPPs. Both the systems are vulnerable to new cyber threats impacting on physical processes in a closed network though these systems of NPPs are isolated from real world internet. However, Stuxnet provides an example of blended attack covering cyber and physical processes that targets nuclear facilities though they are isolated from real world internet connection; where automated controller system thought the centrifuges(controlled process) were spinning at a slower speed than they actually were, and issued an increase speed command when the centrifuges were already spinning at maximum speed which led to equipment damage(concern officials probably wanted to prevent that loss; Stuxnet occurrence at Natanz Nuclear Facility, Iran in June 2010, October 2011, May 2012). Hence, both the digital I&C systems and PPS of NPPs pose a closed cyber physical systems which are critical for safe, enhance performance, convenient maintenance and precise operation. However, NPPs safety analysis methods do not consider these cyber physical systems and also in the cyber security analysis, cyber security vulnerabilities does not often consider as critical, because their effects on the physical processes are not fully understood. Furthermore, literatures in this regards, reveal that several authors have studied the potential impact of security related threats on the safety of digital critical assets of nuclear facilities and highlight the importance of analyzing safety and security risks together (Kornecki and Zalewski, 2010). Therefore, concerns about approaches for NPPs that consider safety and cyber security analysis together are a primary need. Hence, this paper aims to analyze through considering the joint effect of cyber security and safety on NPPs that lead to major accidents. Consequently, this paper proposes a novel STPA-SafeSec methodology to providing a comprehensive analysis of safety and cyber security. The findings shed new light on straightforwardness of regulatory system that help to incorporating additional safety design features as well as to contributing mitigation strategy planning development for the emerging cyber threats in building sustainable cyber physical system at NPPs. Finally, this paper discusses

the implications of the findings for research and practice.

Gender

State

Bangladesh

Author: Dr HOSSAIN, Md. Dulal (Bangladesh Atomic Energy Commission)

Co-authors: Dr ALAM, Md. Mahbub (Bangladesh Atomic Energy Commission); Mr ISLAM, Md. Shamimul (Bangladesh Atomic Energy Commission)

Presenter: Dr HOSSAIN, Md. Dulal (Bangladesh Atomic Energy Commission)

Track Classification: CC: Nuclear safety and security interfaces