INTEGRATED SAFETY AND CYBER SECURITY ANALYSIS FOR BUILDING SUSTAINABLE CYBER PHYSICAL SYSTEM AT NUCLEAR POWER PLANTS: A SYSTEMS THEORY APPROACH

MD. DULAL HOSSAIN
Bangladesh Atomic Energy Commission
Savar, Dhaka, Bangladesh
Main and Presenting Author
Email: edhossain@baec.gov.bd

MD. MAHBUB ALAM
Bangladesh Atomic Energy Commission
Savar, Dhaka, Bangladesh

MD. SHAMIMUL ISLAM
Bangladesh Atomic Energy Commission
Savar, Dhaka, Bangladesh

Abstract

Nuclear power plants (NPP) install digital instrumentation and control (I&C) systems and physical protection systems (PPS) for its safe, 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, the 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 on a large variety of systems today, including nuclear power plants. In the same way, extended STPA can provide a powerful foundation for cyber security analysis. In the context, the study proposes 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 through identifying digital hazards. The application of the novel STPA-SafeSec methodology is illustrated using a case study of a risk scenario in a nuclear facility. Finally, the paper discusses the implications of the findings for research and practice.

1. INTRODUCTION

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. The figure 1 shows the safety and non-safety I&C systems in NPPs (Adapted from Song, J. G., 2012) [1]. 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.

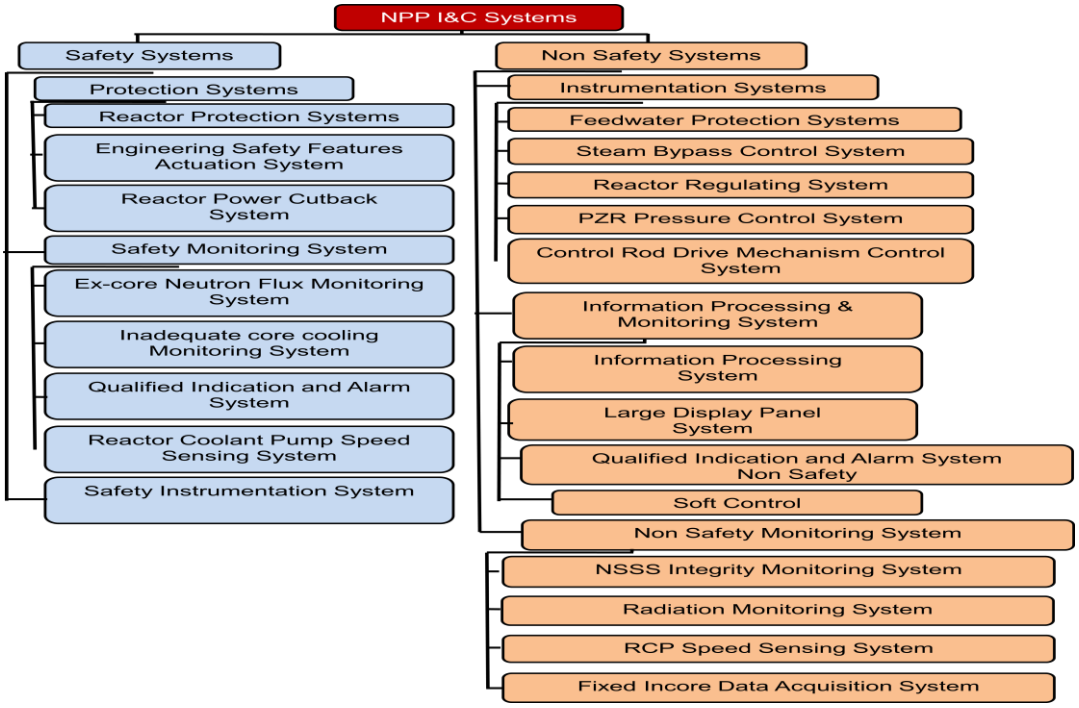

FIG. 1 Safety and Non-Safety I&C Systems in NPPs (Adapted from Song, J. G., 2012) [1]

In the context, 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. Therefore, the study, proposed an integrated approach to provide a comprehensive analysis of safety and cyber security through identifying digital hazards. The figure 2 shows the basic digital I&C systems in NPPs (Adapted from Vesely, W.E., 1998) [2].

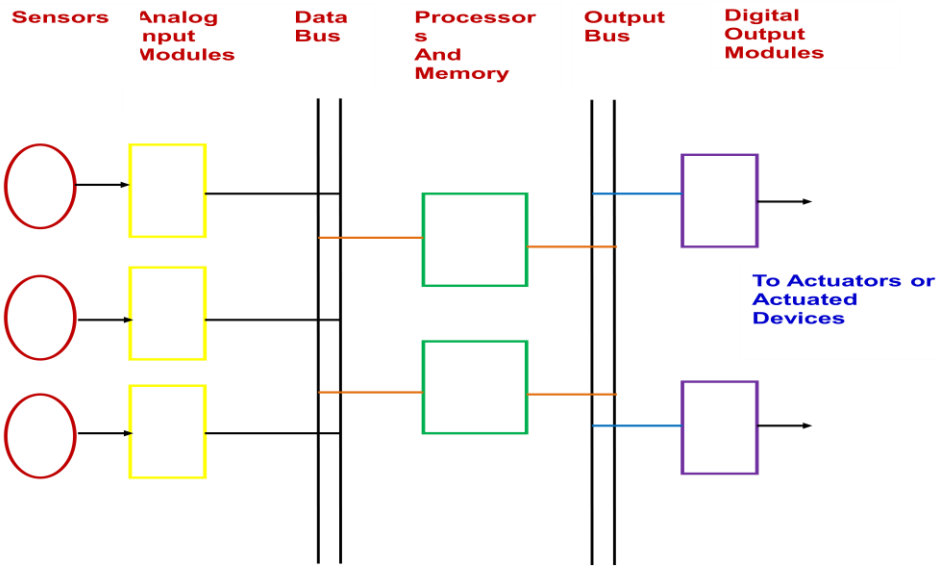

FIG. 2 Basic Digital I&C Systems in NPPs (Adapted from Vesely, W.E., 1998) [2]

2. THEORETICAL FRAMEWORK

The theoretical foundation lays on systems theory which signifies the nature of a complex system. In the context, systems theory represents a framework of investigation that later appropriated as Systems-Theoretic Processes Analysis (STPA). STPA is used on a large variety of systems today as a unique safety analysis approach, including nuclear power plants [3, 4, 5]. On the other hand, extended STPA can provide a powerful foundation for cyber security analysis [3, 5]. The figure 3 shows Design Basis Threat (DBT) for cyber security (Adapted from IAEA Cyber DBT working group).

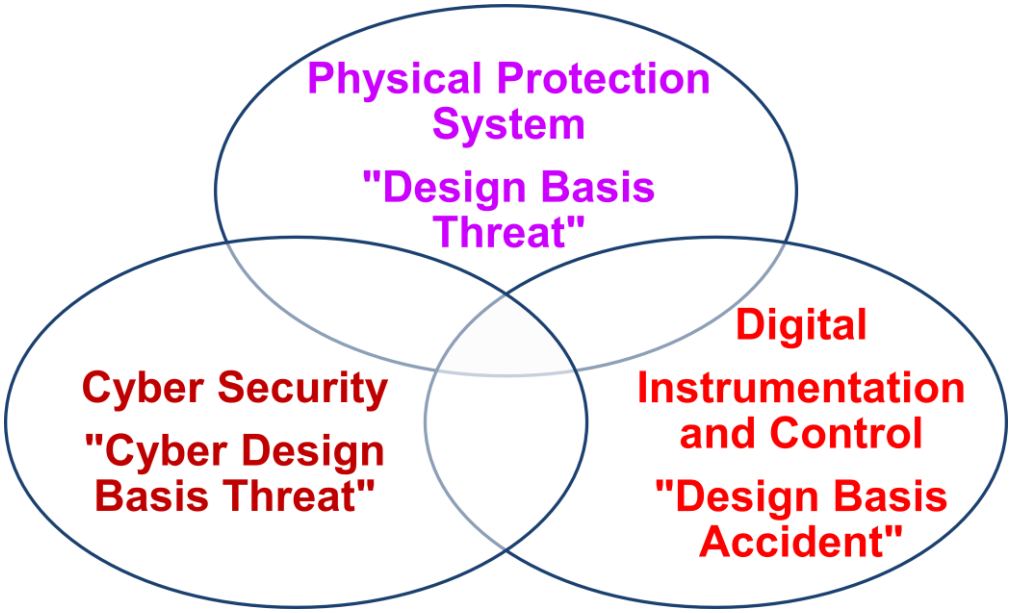

FIG. 3 Design Basis Threat (DBT) for Cyber Security
(Adapted from IAEA Cyber DBT working group)

Therefore, the paper develops an integrated approach of safety and cyber security analysis at nuclear power plants based on systems theory. Finally, the study proposes to combine STPA-Safety and STPA-Security methodology for building sustainable cyber physical system at NPPs. The proposed integrated STPA-SafeSec model provides a comprehensive analysis of safety and cyber security to identify digital hazards in NPPs context.

3. METHODS, MATERIALS AND RESULTS

NPPs safety analysis methods do not consider the 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 [6]. The figure 4 shows NPPs I&C systems threats hierarchy (Adapted from Rahat, M., 2016) [7].

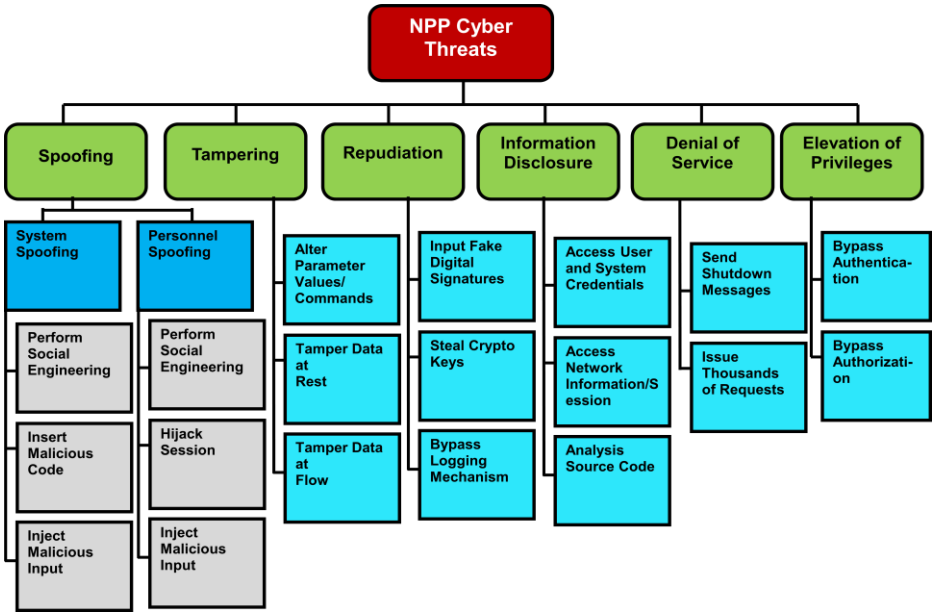

FIG. 4 NPP I&C Systems Threats Hierarchy (Adapted from Rahat, M., 2016) [7]

Therefore, concerns about approaches for NPPs that consider safety and cyber security analysis together are a primary need. Hence, the paper aims to analyze through considering the joint effect of cyber security and safety on NPPs through identifying digital hazards.

4. CONCLUDING REMARKS

The paper proposes a novel STPA-SafeSec model to identify digital hazards in NPPs through a comprehensive analysis of safety and cyber security. The findings shed new light on straightforwardness of regulatory system and help to incorporating additional safety design features. The integrated assessment results of the analysis can incorporate to developing DBT both for physical and cyber. The results also contribute mitigation strategy planning development for the emerging cyber threats in building sustainable cyber physical system at NPPs. Finally, the full fledged study discusses the implications of the findings for research and practice.

5. REFERENCES

[1] Song, J.G, Lee, J.W., Lee, C.K.,Kwon, K.C.,Lee, D.Y, "A Cyber security risk Assessment for the Design of I&C Systems in Nuclear Power Plants" Journaal of Nuclear Engineering and Technology, Vol. 44, No. 8, 2012

[2] Vesely, W.E. "Digital I&C Systems in Nuclear Power Plants Risk-Screening of Environmental Stressors and a Comparison of Hardware Unavailability With an Existing Analog System" January 1998 Brookhaven National Laboratory, U.S. NRC Washington, DC 20555-0001, https://www.osti.gov/servlets/purl/574196

[3] Friedberg, I., McLaughlin, K., Smith, P., Laverty, D., Sezer, S. "STPA-SafeSec: Safety and security analysis for cyber-physical systems" Journal of Information Security and Applications, Vol. 34, pp.183–196, 2017

[4] Young, W, Leveson, NG, "An integrated approach to safety and security based on systems theory" Commun ACM, Vol. 57, No. 2, pp. 31–35, 2014

[5] Young, W, Leveson, N, "Systems thinking for safety and security" In: Proceedings of the 29th Annual Computer Security Applications Conference on -ACSAC '13, ACM Press, New York, New York, USA., pp. 1–8, 2013.

[6] Kornecki, A. J., Zalewski, J. "Safety vs. Security in Industrial Control" 2010, https://www.academia.edu/3199218/Safety_and_security_in_industrial_control

[7] Rahat, M., "Assessment of Cyber Security Challenges in Nuclear Power Plants *Security Incidents, Threats, and Initiatives"* Report GW-CSPRI-2016-03, 2016. https://cspri.seas.gwu.edu/sites/g/files/zaxdzs1446/f/downloads/GW-CSPRI-2016-03%2BMASOOD%2BRahat%2BNuclear%2BPower%2BPlant%2BCybersecurity_0.pdf