Contribution ID: **596** Type: **Poster**

National Nuclear Security Regulation: Overview of Nuclear Cyber Security Requirements for NPPs

Abstract
We are living in a digital and information-driven age and need to store information related to virtually every aspect of our lives, nuclear information included. For computer system to be reliable and secure in nuclear facilities, unauthorized event changes must be prevented (which means maintaining - confidentiality), field device inputs and outputs must remain immutable throughout their usable lifetime (which means maintaining - integrity), and all component parts should remain in an operable state (which means maintaining - availability).The dynamic and complex nature of cyber threats has made it a serious challenge to secure computer systems in nuclear facilities. A number of varied cyber security services, policies, mechanisms, strategies and regulatory frameworks have been adopted , including: confidentiality, integrity, availability, non-repudiation, encipherment, defence-in-depth (DID), design basis threat (DBT), IAEA technical guidance documents such as: GS-R-1, GS-R-2, NSS13, NSS17, NST036, NST045, and NST047, IEEE standard 7-4.3.2-2010, NIST SP 800-53, NIST SP 800-53, NIST SP 800-82, NEI 04-04, NEI 08-09 and country-specific requirements such as: 10 CFR 73.54, RG 5.71 (U.S.NRC), KINS/RG-N08.22 (South Korea). However, threats remain persistent. This paper is aimed at providing an overview of regulatory standards and frameworks governing cyber security in nuclear power plants (NPPs) around the world, regulatory requirements and global best practice recommendations for nuclear cyber security, and strategies to prevent and counteract threats. This study is imperative as Nigeria prepares to join the league of countries with operational nuclear power plants and research reactors following approval and adoption of the nuclear power programme roadmap in 2007 and contract signing with Rosatom of Russia for NPP and research reactor construction.

Keywords: Cyber security, nuclear security, nuclear power plants, critical digital assets

Gender

Male

State

Nigeria

Author: Mr ARINZE, Uchechukwu (Information and Communication Technology (ICT) Unit, Department of Radiological Safety, Nigerian Nuclear Regulatory Authority (NNRA), South East Zonal Office, Enugu, Enugu State.)

Co-authors: Dr ENEH, Agozie (Computer Science Department, Faculty of Physical Sciences, University of Nigeria, Nsukka (UNN), Enugu.); Prof. LONGE, Babatunde Olumide (Department of Information Systems, School of Information Technology & Computing, American University of Nigeria (AUN), Yola, Adamawa State.)

Presenter: Mr ARINZE, Uchechukwu (Information and Communication Technology (ICT) Unit, Department of Radiological Safety, Nigerian Nuclear Regulatory Authority (NNRA), South East Zonal Office, Enugu, Enugu State.)