Contribution ID: **642** Type: **Poster**

CONSEQUENCES OF CYBER-ATTACKS IN A NUCLEAR SECURITY SYSTEM OF A BRAZILIAN NUCLEAR POWER PLANT

CONSEQUENCES OF CYBER-ATTACKS IN A NUCLEAR SECURITY SYSTEM OF A BRAZILIAN NUCLEAR POWER PLANT

João C. B. Fiel1 and Pedro M.R. dos Santos1

1 Instituto Militar de Engenharia (IME)
Praça General Tibúrcio, 80 - Urca
22290-270 Rio de Janeiro, RJ, Brazil
fiel@ime.eb.br

ABSTRACT

This paper aims to describe an assessment of cyber-attacks impacts in the effectiveness of the security system of a hypothetical Brazilian facility that comprises a small modular reactor of iPWR type. Performance data have been extracted from several sources on IAEA. The methodology uses a performance-based approach to calculate baseline system probability of effectiveness (PE) as well as the decrease on PE under the interference of cyber threat. Some attack scenarios are postulated in order to evaluate the influence of this threat in a security project. The scenarios postulated includes credible cyber-attacks in the computational systems that controls exterior, interior, position and fence sensors. Under these simple scenarios, the probability of interruption (PI) of an outsider would decrease to low levels. Consequently, in most of scenarios, even under total probability of neutralization (PN), it would not be possible to mitigate the threat timely, making possible to carry out a blended attack. From the results obtained by this paper, it is possible to easily identify the security level that must be associated to the cyber-systems in the nuclear facility, as indicated by the NSS-17G.

Gender

State

Brazil

Primary authors: BATISTA FIEL, Joao Claudio (Military Institute of Engineering); M.R. DOS SANTOS, Pedro (Instituto Militar de Engenharia)

Presenter: BATISTA FIEL, Joao Claudio (Military Institute of Engineering)

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