World Academy of Science, Engineering and Technology
International Journal of Nuclear and Quantum Engineering
Vol:16, No:11, 2022

# Resilient Machine Learning in the Nuclear Industry: Crack Detection as a Case Study

**Authors :** Anita Khadka, Gregory Epiphaniou, Carsten Maple

**Abstract :** There is a dramatic surge in the adoption of machine learning (ML) techniques in many areas, including the nuclear industry (such as fault diagnosis and fuel management in nuclear power plants), autonomous systems (including self-driving vehicles), space systems (space debris recovery, for example), medical surgery, network intrusion detection, malware detection, to name a few. With the application of learning methods in such diverse domains, artificial intelligence (AI) has become a part of everyday modern human life. To date, the predominant focus has been on developing underpinning ML algorithms that can improve accuracy, while factors such as resiliency and robustness of algorithms have been largely overlooked. If an adversarial attack is able to compromise the learning method or data, the consequences can be fatal, especially but not exclusively in safety-critical applications. In this paper, we present an in-depth analysis of five adversarial attacks and three defence methods on a crack detection ML model. Our analysis shows that it can be dangerous to adopt machine learning techniques in security-critical areas such as the nuclear industry without rigorous testing since they may be vulnerable to adversarial attacks. While common defence methods can effectively defend against different attacks, none of the three considered can provide protection against all five adversarial attacks analysed.

**Keywords :** adversarial machine learning, attacks, defences, nuclear industry, crack detection
**Conference Title :** ICNST 2022 : International Conference on Nuclear Security and Technology
**Conference Location :** London, United Kingdom
**Conference Dates :** November 18-19, 2022