

Machine Learning -based process control monitoring and cyber security: Similarities, conflicts and limitations

Analog control systems are being replaced by digital Instrumentation and control systems in the nuclear power plant control consoles to improve reliability, availability and enhance the decision-making process. The introduction of digital systems has produced a network of reactor safety components with Programmable Logic Controllers (PLCs), sensors, valves, and breakers. By association, the vulnerabilities in these digital systems have been inadvertently transferred to the safety systems and these cyber vulnerabilities could quickly become safety issues. Consequently, when a plant goes into crises mode, the swift response of the operator is highly desirable. In nuclear plants, two most commonly cited causes of abnormality are system faults and cyber attacks. To address these issues, many machine learning abnormality detection techniques have been proposed for a wide range of key systems in nuclear power plants. However, many reported cyber-attacks carried out on process control systems usually appear as system failure or fault injection, and these two "abnormal occurrence" initiating event could sometimes have similar signatures. That is, cyber-attacks could be easily mistaken for a random system fault. It is also observed that, safe for the dataset used in training these machine learning algorithms, the techniques used for fault detection and cyber security are fundamentally similar. In a complex system such as nuclear plant, it is pertinent to develop a robust but distinct detection system with the capability to explore the similarity in signature to differentiate between the two events, as the consequence of each of them, the required response, and the overall effect to system safety are entirely different.

This paper reviews proposed machine learning-based abnormality detection tools, techniques, limitations, issues, challenges and the status of their application in NPP. We also discuss the similarities, conflicts and the limitation of the machine learning tools used for fault diagnosis and cybersecurity in the protection of complex systems such as NPP, and the need to establish clear differences between them. Sources of the dataset used in training and testing the machine learning algorithm are described and their limitations are discussed. Some proposed methodology to integrate security algorithms to enhance safety tool to include malicious attack detection in NPP is also reviewed. Finally, future direction and recommendations for the efficient distinction of these incidences are presented.

Gender

Male

State

China

Author: Mr AYODEJI, Abiodun (Nigeria Atomic Energy Commission/Harbin Engineering Univeristy)

Co-author: Prof. LIU, Yong-kuo (Harbin Engineering University)

Presenter: Mr AYODEJI, Abiodun (Nigeria Atomic Energy Commission/Harbin Engineering Univeristy)

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