Contribution ID: **318** Type: **Paper**

Consideration of Artificial Intelligence for Cybersecurity Aspects of I&C Systems

After two extended up and down periods in the historical development of Artificial Intelligence (AI) during the last decades, since a few years, many AI solutions have become inherent components in several industrial business domains. We will briefly analyze how AI came to be where it is now and what boundary conditions have to be met in order to be able to apply AI. Yearly AI competitions allow for an outlook towards what performance the AI solutions are heading to. We will look at how AI is considered for security aspects in Industry 4.0 and how this can be applied for the nuclear domain, especially for Safety I&C, Operational I&C and Electrical Power Systems (EPS).
According to our focus, we will indicate what types of Machine Learning (ML) can be applied and what key security challenges have to be considered. The key AI supported concepts that will be addressed include: identification and authentication with AI support, AI supported anomaly detection in data streams and AI based identification of potential malware.
Beyond these AI based technologies for the implementation of selected security control, in two main sections we will address the genesis of new attack vectors through AI and the use of AI to improve the resilience of Safety I&C, OT and IT environments against sophisticated attacks.
Finally, we will also address the integration of AI approaches with traditional approaches from implementing and validating security controls and for attack tree analysis. This is an ongoing development where decisions on the effort for supervised Machine Learning (identification of representative vectors, tagging of artefacts, tagging of relations) or unsupervised ML has to be balanced with the effort for validating the results obtained via involved AI algorithms. With a focus on security testing the validation of representativeness and coverage of the AI based results remains an important challenge for ongoing R&D. The strength of the AI supported protection may have an impact to nuclear safety (due to potentially remaining residual risks), a topic that will be outlined but not elaborated in detail in this paper.

Gender

Female

State

Germany

Primary author: Ms BEN ZID, Ines

Co-authors: Ms LOU, Xinxin; Dr WAEDT, Karl

Presenter: Ms BEN ZID, Ines

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