Contribution ID: **41** Type: **Poster**

Industrial Cybersecurity and Machine Learning*

Friday 13 September 2024 09:20 (20 minutes)

Nowadays, we are dealing with the development of industrial technologies that bring numerous benefits, but also new threats. Many technological industries are focusing on Industry 4.0, where digitization and process automation are key, and the emerging cyber threats are becoming an increasingly significant problem. As the industry develops, cyber threats evolve. In industry, this requires constantly adapting defence strategies. However, by using machine learning, we can better predict, detect and neutralize threats, protecting key industrial resources from the growing number of cyberattacks.

Increasingly, attention is being paid to using elements of artificial intelligence (AI) for industrial security purposes. As mentioned earlier, this is becoming more important as industrial systems become more complex and exposed to various cyber threats. Machine learning is noteworthy in this context, as it can significantly enhance the security of these systems by automatically detecting anomalies and threats in real time. For example, ML models can analysis data from sensors and PLCs (Programmable Logic Controllers), identifying unusual patterns that may indicate potential attacks or failures.

Today, industry cannot work without PLC controllers, which are a main elements of process automation systems. With technological improvement, need to secure these devices from increasingly sophisticated cyber threats is growing. Machine learning appears to be a tool that can significantly enhance the security of PLC-based systems. Additionally, ML properties can be utilized for predictive maintenance of production processes, allowing for the prediction and prevention of equipment failures, thus minimizing downtime and repair costs.

At the same time, ML systems must be secured against attacks that can manipulate input data to distort the models. Cybersecurity in ML also involves protecting data privacy through techniques that allow for model training without revealing operational data. An integrated approach to cybersecurity, which includes both traditional methods and modern ML techniques, is crucial for protecting industrial infrastructure. Moreover, automating security with additional tools can increase efficiency in responding to threats.

As ML technology evolves, it is essential to continually research and update protection strategies to keep up with the changing threat area. Finally, educating and training security teams about ML-specific threats is key to effectively protecting industrial systems.

Therefore, the goal of this work is to comprehensively present the role of machine learning in improving cybersecurity in industry, considering both the benefits that this technology brings and the challenges that need to be overcome to effectively protect industrial systems from modern cyber threats.

*This work is financed from the research Grant No. 0211/SBAD/0123.

Authors: Dr POCHMARA, Janusz (Poznan University of Technology); ŚWIETLICKA, Aleksandra (Poznan University of Technology); Dr KOLANOWSKI, Krzysztof (Poznan University of Technology)

Presenters: Dr POCHMARA, Janusz (Poznan University of Technology); ŚWIETLICKA, Aleksandra (Poznan University of Technology); Dr KOLANOWSKI, Krzysztof (Poznan University of Technology)

Session Classification: Session 6 - Poster Session B