ФОНД НАУЧНИ ИЗСЛЕДВАНИЯ
Министерство на образованието и науката

Information for research project

Call: Competition for financial support of basic research projects – 2020
Main scientific area: Technical sciences/ Information and communication technologies
Contract No: КП-06-Н47/7
Initial date and duration of the project: 15.12.2020 – 15.12.2023
Project title: Possibility Investigation of Increasing the Cybersecurity of the Systems in Industry 4.0 using Artificial Intelligence
Research organization: Technical University of Sofia
Partner organizations: -
Principle investigator: ***Prof. PhD Eng. Roumen Trifonov***

Abstract of the research project

In the overall development of the digital society in recent years, so-called digital transformation of the industry occurs as a result of the increasing penetration of the Internet of Things (IoT), robotics, 3D printing, cloud solutions, and artificial intelligence-based cognitive technologies. All these technologies in a whole form the Industry 4.0, driven not only by design and production, but also by relationship of the production with the market and consumers.

In Industry 4.0 achievement of a sufficiently high level of cybersecurity is crucial for the reliable effective functioning of industrial systems. This is especially evident in the so-called "Critical infrastructures" providing vital functions of the economy and society (energetics, transport, etc.). Modern attacks through the Internet are complex, organized, and use a wide range of "Advanced Persistent Threats" with a long-hidden period. Often they are targeted at high value but poorly protected targets/objects and can easily escalate from a cyber incident to a cyber crisis.

In these conditions the overwhelming majority of experts agree that traditional methods of protection are already poorly productive and that a qualitative transition to new instruments is needed. One of the priority areas of this transition is the widespread use of artificial intelligence methods.

The purpose of the present project is to systematize, analyze, experiment and evaluate the different types of artificial intelligence applications in cybersecurity of industrial systems in Industry 4.0, especially their cyber-physical components, through which self-regulatory networks for spatially distributed production are created. As a result of this work, the most perspective methods for the national practice have to be selected and recommendations should be drawn up for their use.

The main hypothesis of the ideology, which contains in the project proposal, is the tendency to build multi-layered protection for consumers or operators of industrial networks, the modern multilayer defense methods adequately to counter to the Advance Persistent Threats (ART).

The scientific research in the project proposal is fundamental, because it is not about the evaluation and selection of certain specific technical solutions but the analysis and comparative evaluation of different methods and areas of artificial intelligence and related fields.

During the implementation of the project, it is planned to use research methods, which will activate a wide range of control, laboratory and technological equipment for the necessary studies with simulator and in experimental or real industrial environment. In order to carry out the tests, a prototype of an Industrial System will be created, on which all tests and experiments will be conducted.

The project results will be based on the analysis of the specific for industrial systems cyber-attacks and the application of artificial intelligence methods for counteraction or their timely localization. An optimal approach to prevent the detection of cyber-attacks will be proposed.

All the scientific results from these activities will lead to new knowledge in the field of information and communication technologies for increasing the level of cyber security of industrial systems in Industry 4.0 using artificial intelligence.

The research results of the project will be shaped in the form of scientific articles, which will be sent to scientific publications, refereed and indexed in the world secondary literature, as well as and/or in the publications with Impact Factor, IF (Web of Science) and/or Impact Rank SJR (SCOPUS), as well as presented in national and international scientific conferences.