Security of Industrial Control Systems: challenges, trends and innovative solutions

Assoc. Prof. Emil PRICOP
(Head of) Automatic Control, Computers & Electronics Department
Petroleum-Gas University of Ploiesti, Ploiesti, Romania
emil.pricop@upg-ploiesti.ro

Control systems are key components enabling the functioning of any industrial infrastructure, being it an energy production and distribution facility, a petrochemical plant, an automotive factory or a nuclear plant. Moreover, control systems coordinate the correct functioning of medical equipment, HVAC systems, and even autonomous or classical cars. The increased complexity and connectivity of Industrial Control Systems (ICS) enabled them to be a key component of Industry 4.0 infrastructures, by becoming nodes in a big automation cloud.

The connectivity of control systems allows real-time monitoring, remote operation, but at the same time makes them an attractive target for various categories of attackers. There were signals of an increasing number of cyberattacks on ICS, as presented in the reports of renowned cybersecurity companies and research laboratories. The attack scope was to have a significant economic and societal impact, mainly by interrupting the functioning of various industries.

In this context, ICS security is becoming a priority of systems manufactures, owners and operators. The security of industrial control systems should focus on both physical access control and protection against cyber threats. The main challenge associated with this approach is to maintain a high-security level without affecting the performances and the operating procedures of the ICS.

The threats and vulnerabilities are dynamically changing and target all the levels of a hierarchical ICS, ranging from field level equipment (sensors, actuators), SCADA systems to ERP and enterprise level. In this context, a security assessment must be pursued for each level and even each specific device. The keynote lecture will present vulnerabilities related to each ICS level.

The vulnerabilities are the ways attackers try to use to access the protected assets. An effective security policy will also assess the potential attackers and their interest in the system. The keynote lecture focuses on the usage of honeypots and honeynets as an efficient method for recording relevant data regarding the attackers' interest in the ICS components and even for tracking the "modus operandi".

The keynote lecture concludes with innovative solutions and recommendations to increase the security of the industrial control systems.