**Abstract**

*Security evaluation method of industrial network components on the example of programmable logic controllers.*

**Author**: Dariusz Rogowski, MSc

Industrial Automation and Control Systems and their components are becoming increasingly a target of cyber attacks that permeate into industrial networks from enterprise networks. It is happening due to the deeper integration of industrial networks with enterprise management systems.

For this reason, the problem of efficient protection of control devices, which in many cases control elements of critical infrastructures, is becoming more serious. Entrepreneurs want confirmation and assurance that the applied security measures will work.

The doctoral thesis solves the problem of the availability of security evaluation methods for industrial components. The author developed a method for IT security evaluation of industrial automation and control systems, thus fulfilling the primary goal of the research work.

The method relies on the international Common Criteria standard (ISO/IEC 15408) and the Common Evaluation Methodology, CEM (ISO/IEC 18045), dedicated to IT security evaluation. The standard is a source of techniques for creating assurance based on controlled, rigorous processes of developing, documenting, and testing the product. As the only standard, it introduces the so-called assurance measures in the form of an Evaluation Assurance Level (EAL).

The problem is that the CC standard contains security evaluation criteria typical for IT solutions. At the same time, it is an advantage because threats to industrial devices are of an IT nature, and they should be treated alike in this context. This problem was solved by selecting industrial security requirements as the source for adapting the CC standard to specific industrial needs. The IEC 62443 family of standards was selected as it defines the requirements and processes for the secure IACS components implementation and maintenance.

Consequently, the Common Criteria requirements were supplemented with characteristics specific to industrial components. Then these requirements were included in the evaluation method. They consist of security assurance requirements, functional requirements, and evaluators' actions used for evaluating those requirements.

Next, the security evaluation method for IACS, which implements the adapted CC and CEM requirements, was validated. The validation consisted in verifying the developed requirements. It was based on the pilot security evaluation of the programmable line distance protection controller carried out in the security evaluation laboratory. The controller was tested for compliance with industrial security requirements. The same industrial requirements were used in the adapted evaluation method.

Validation of the method allowed to confirm the following thesis of the doctoral dissertation: *The Common Criteria methodology can be applied to the security evaluation of industrial network components after its adaptation to the needs and realities specific to the operational environment of these components.*

The security evaluation method developed for IACS is a universal tool, integrating the IT and industry worlds, allowing the joint evaluation of their security measures and increasing the evaluation assurance level.