Advances in Reliability, Safety and Security

ESREL 2024
Collection of Extended Abstracts

First Experiences In Cybersecurity Evaluation And Certification Of IACS Components

Jacek Bagiński, Rafał Kurianowicz

Łukasiewicz Research Network – Institute of Innovative Technologies EMAG, Katowice, Poland

Keywords: industrial automation and control, IACS, cybersecurity, requirements, evaluation, IT Security Facilities,

The work presents a description of the practical validation of the method for the security evaluation and certification of industrial network components. The results of the work were verified in practice during a pilot evaluation of an industrial controller used in the power industry and used to obtain accreditation for the laboratory and the Certification Body (CB) operating within the Łukasiewicz-EMAG institute. Both the laboratory and the CB were to be the first entities of this type by Polish Centre for Accreditation (PCA) in the field of testing and certification of the IT security of Industrial Automation and Control System (IACS) components.

The work presents the use case and describes the experience of establishing an accredited laboratory and Certification Body for IACS components in accordance with the IEC 62443 industry standard (IEC 62443-4-2, 2019), and the methodology (CCRA CEM, 2017).

Accredited Laboratory - IT Security Facility (ITSEF) for assessing products in terms of compliance with the requirements of the so-called Common Criteria for assessing the security of IT products already exists in Łukasiewicz-EMAG. Activities carried out as part of the project enabled the laboratory to be prepared for testing solutions in the area of Industrial Internet of Things (IIoT), IACS, and accreditation could be extended to include an assessment in this area.

The work shortly lists the regulatory basis, materials, methods analysed on the basis of which the laboratory, processes and required documentation were developed: NIST Special Publication 1800-32 (McCarthy, et al., 2022), NIST Special Publication 800-82 (Stouffer, et al., 2023), SESIP methodology based on the ISO/IEC 15408-3 (SESIP, 2021), adapted to Internet of Things (IoT) assessment, TeleTrust (Glemser, et al., 2019) evaluation method for the IEC 62443-4-2 of the IT Security Association Germany, recommended by ERNCIP – European Reference Network for Critical Infrastructure Protection, other industry certification groups (IIC, 2023), (ioXt, 2021), (CTIA, 2023). A justification for the selection of the main standard for product evaluation.

The assessment process was to be in line with the basic assumptions of the ITSEF assessment functioning in the ITSEF laboratory for the ISO/IEC 15048 (Common Criteria) standard (ISO/IEC 15408-1, 2009) (ISO/IEC 15408-2, 2008) (ISO/IEC 15408-3, 2008), but the process had to be simplified, adapted to the assessment in a shorter time.

When starting these activities in the laboratory (according to the method proposed in (Rogowski, 2023), experience from the implementation of the lightweight certification schemes in other European countries was also taken into account: LINCE (CCN, 2022), BSZ (BSI, 2023) and CSPN (ANSSI, 2023), as well as different industry specific standards and evaluation programs.

The results of the case are shortly presented, experience from preparing a laboratory for the evaluation of IACS components' security functions, as well as establishing the certification body.

The main assumptions regarding the preparation of the template and the required content of the Security Target for Industrial Component (STIC) document (among other - security problem definition) are presented. Then, based on the STIC document and other documentation, and tests of the component in the laboratory, a report is prepared. The report is an input element for the certification body. It may issue a certificate of compliance of the component with the requirements of the standard (IEC 62443-4-2, 2019).

The description of the first evaluation was shortly prepared. The evaluation was performed for the Target of Evaluation - the industrial PLC (Programmable Logic Controller) - programmable line distance protection controller for power substations.

Finally, conclusions from the implementation of the adopted method, experience gained from the project and expected opportunities for further development to build fast cybersecurity certification programs for IoT, IIoT, Data Centres, Cloud Computing and IACS devices.

Acknowledgements

The contribution presents the results of the R&D project “Cybersecurity evaluation and certification – smart certification schemes “(CyberBEAM, 2021-2024). The project is financed by the National Centre for Research and Development (NCBR) within the program CyberSecIdent (Grant No. CYBERSECIDENT/489595/IV/NCBR/2021).

References

ANSSI 2023. Évaluer les produits et services – Certification et qualification. Available at: https://cyber.gouv.fr/evaluer-les-produits-et-services-certification-et-qualification (accessed 28 12 2023).

BSI 2023. Beschleunigte Sicherheitszertifizierung (BSZ). Available at: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Beschleunigte-Zertifizierung/beschleunigte-zertifizierung.html

CCN 2022. Definición de la Certificación Nacional Esencial de Seguridad (LINCE). Guía de Seguridad de las TIC, Issue CCN-STIC 2001.

CCRA CEM 2017. Common Methodology for Information Technology Security Evaluation – Evaluation Methodology. CCMB-2017-04-004, Version 3.1, Revision 5.

CTIA 2023. CTIA Certification. Available at: https://ctiacertification.org/ (accessed 28 12 2023).

CyberBEAM 2021-2024. Łukasiewicz-EMAG - szczegóły projektów. Available at: https://www.emag.lukasiewicz.gov.pl/pl/szczegoly-projektow (accessed 28 12 2023).

Glemser, T., Heyde, S., Muehlbauer, H. 2019. TeleTrust Evaluation Method for IEC 62443-4-2, Security for Industrial Automation and Control Systems, Berlin: IT Security Association Germany (TeleTrusT).

IEC 62443-4-2 2019. Security for Industrial Automation and Control Systems, Part 4-2: Technical Security Requirements For IACS Components. International Electrotechnical Commission.

IIC 2023. Industry IoT Consortium. Available at: https://www.iiconsortium.org/# (Accessed 28 12 2023).

ioXt 2021. Available at: https://www.ioxtalliance.org/ (accessed 28 12 2023).

ISO/IEC 15408-1 2009. Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.

ISO/IEC 15408-2 2008. Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components.

ISO/IEC 15408-3 2008. Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components.

McCarthy, J. et al. 2022. Securing Distributed Energy Resources: An Example of Industrial Internet of Things Cybersecurity.

Rogowski, D. 2023. Security evaluation method of industrial network components on the example of programmable logic controllers (PhD Dissertation). Gliwice

SESIP 2021. Security Evaluation Standard for IoT Platforms (SESIP) Methodology. GlobalPlatform.

Stouffer, K. et al. 2023. Guide to Operational Technology (OT) Security.