Advances in Reliability, Safety and Security

ESREL 2024
Collection of Extended Abstracts

IT/OT Cybersecurity Evaluation – State Of Art Summary

Andrzej Białas

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

Keywords: IIoT, IACS, security evaluation, security certification, Cybersecurity Act

The components of Industrial Automatic and Control Systems (IACS), as well as intelligent sensors, instruments and autonomous devices connected through the internet to industrial applications embraced by the term IIoT (Industrial Internet of Things) represent specific IT products and strongly require security assurance. Security assurance is growing when the right development methodologies are applied and IT product security is independently evaluated and then certified.

There are many national security evaluation schemes based on the Common Criteria (CCRA, 2023). However, they are often not ready to evaluate numerous and varied IACS/IIoT components that are developed within the information technology domain. For several years, there have been methods developed to solve this problem. Some of approaches already work, while the most comprehensive, elaborated for a broad (European/world) audience ones are under development. There is a market need – the evaluation and certification process should be closed in the assumed time and the certificates should be widely recognized.

The publication presents concisely main directions and results of these works.

1. The Regulation (EU) No 2019/881 called the Cybersecurity Act (CSA) (EU, 2019) presents a framework for the establishment of these European cybersecurity certification schemes and their elements e.g.: subject matter and scope, purpose, evaluation methods, references to European or national standards, and many other issues. It specifies 10 security objectives to be included in schemes focused on ICT products, ICT services and ICT processes. It defines security levels BASIC, SUBSTANTIAL and HIGH, related risk to be minimized, and evaluation activities for them. Self-evaluation is possible for the BASIC level.
2. The ERNCIP Report (Theron et al., 2020) is a considerable refinement of the CSA from technical perspective. It includes more details and requirements for the ICCS (IACS Components Cybersecurity Certification Scheme). For each security level, BASIC, SUBSTANTIAL and HIGH, the requirement concerning security documentation and artefacts ought to be delivered to evaluators and evaluation activities are specified. The FITCEM (EN 17640) methodology (CEN/CENELEC, 2022) developed by the CEN/CENELEC JTC13 WG3 is claimed as the first cybersecurity methodology created to meet the European Cybersecurity Act (CSA) (JTSEC, 2023). This flexible methodology can be customized to meet the needs of the different schemes and self-evaluation. Three possible certification paths are considered:
    - based on IEC 62443; IEC 62443-4-2 (EC IEC, 2019) includes security requirements addressed to security features of components, and IEC 62443-4-1 (EC IEC, 2018) concerns security requirements for the IACS component life cycle;
    - based on Common Criteria (CCRA, 2023), (ISO/IEC, 2022a), (ISO/IEC, 2022b);
    - based on a lightweight scheme, which assumes simplified evaluation (security target analysis, installation assessment, documentation review, functional testing, vulnerability analysis and penetration testing), restricted short evaluation time period and relatively lower costs;

3. For IIoT/IoT some company-owned schemes operate, e.g.: the CTIA Cybersecurity Certification Program for IoT devices (CTIA, 2021), the ioXt Alliance (ioXt Alliance, 2024), the Security Evaluation Standard for IoT Platforms – SESIP (GPT, 2021).
4. Leading world organizations work on evaluation methods:
    - the IIoT Component Certification based on the 62443 standard methodology is developed under auspices of the ISA Global Security Alliance and the ISA Security Compliance Institute (GSA-ISA, 2021);
    - IEC TC 65 Industrial-process measurement, control and automation WG 10 is working on the project "IEC TS 62443-6-2 ED1 Security evaluation methodology for IEC 62443 - Part 4-2: Technical security requirements for IACS components" related to the evaluation of IACS components (Forescout, 2020).

The activities of the following institutions are very important: EU legislation bodies (European Commission, Parliament), CCRA (Common Criteria Recognition Arrangement) signatories, ISO (International Organization for Standardization), IEC (International Electrotechnical Commission), NIST (National Institute of Standards and Technology), CEN (European Committee for Standardization), CENELEC (European Committee for Electrotechnical Standardization), SOGIS (Senior Officials Group Information Systems Security), ENISA (European Union Agency for Network and Information Security), and many others.

Acknowledgements

The paper 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) – Grant No. CYBERSECIDENT/ 489595/ IV/ NCBR/ 2021).

References

CCRA. 2023. Common Criteria Portal Home Page. https://www.commoncriteriaportal.org/ (accessed on 17 December 2023).

CEN/CENELEC. 2022. EN 17640:2022 Fixed-time cybersecurity evaluation methodology for ICT product.

CTIA. 2021. Internet of Things (IoT) Cybersecurity Certification. https://ctiacertification.org/program/iot-cybersecurity-certification/ (accessed on 18 December 2023).

EC IEC. 2018. EC IEC 62443-4-1: 2018 Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements.

EC IEC. 2019. EC IEC 62443-4-2: 2019 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components.

EU. 2019. CSA - Cybersecurity Act. REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013.

Forescout Tech. Inc. 2020. How to Effectively Implement ISA 99/IEC 62443. https://www.forescout.com/how-to-effectively-implement-isa-99iec-62443/?utm_source=google&utm_medium=cpc&utm_campaign=ppc_ot_emea&cq_con=119805755693&cq_term=iec%2062443&cq_med=&cq_plac=&cq_net=g&gad_source=1&gclid=CjwKCAiA1-6sBhAoEiwArqlGPowCJmz2d5wiqDFC7QD8ER5x14g84SHIko2xh-nXbt5wuzYnYmOIZhoC-xUQAvD_BwE (accessed on 8 January 2024).

GlobalPlatform Technology. 2021. Security Evalution Standard for IoT Platform. https://globalplatform.org/wp-content/uploads/2021/03/GP_SESIP_v1.0.0.4_PublicRvw.pdf (accessed on 21 December 2023).

Global Security Alliance and the ISA Security Compliance Institute. 2021. IIoT Component Certification Based on the 62443 Standard. ISA, V1.4. https://21577316.fs1.hubspotusercontent-na1.net/hubfs/21577316/2023%20ISA%20Website%20Redesigns/ISAGCA/PDFs/ISCI%20and%20ISAGCA%20Joint%20IIoT%20Study%20-%20Full%20Study-5.pdf (accessed on 8 January 2024).

ioXt Alliance. 2024. ioXt – Internet of secure things. https://www.ioxtalliance.org (accessed on 8 January 2024).

ISO/IEC. 2022a. ISO/IEC 15408:2022 Information security, cybersecurity and privacy protection Evaluation criteria for IT security (Part 1 to Part 5).

ISO/IEC. 2022b. ISO/IEC 18045:2022a. Information security, cybersecurity and privacy protection Evaluation criteria for IT security. Methodology for IT security evaluation.

JTSEC. 2023. https://www.jtsec.es/blog-entry/119/fitcem-en-17640-the-first-cybersecurity-methodology-created-to-meet-the-european-cybersecurity-act-csa (accessed on 9 January 2024).

Theron, P., Ruiz-Gualda, J.F. et.al. 2020. Recommendations for the Implementation of the Industrial Automation & Control Systems Components Cybersecurity Certification Scheme (ICCS), Ispra: European Commission.

Disaster preparedness, mitigation and response