Advances in Reliability, Safety and Security, Part 10 – Kołowrocki, Kosmowski (eds.)
 ISBN 978-83-68136-22-7 (printed), ISBN 978-83-68136-09-8 (electronic)

Advances in Reliability, Safety and Security

ESREL 2024
Monograph Book Series

First Experiences In Cybersecurity Evaluation And Certification Of IACS Components

Jacek Bagiński, Rafał Kurianowicz

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

Abstract

The article presents a description of the practical validation of the method for the security evaluation of industrial network components, proposed in (Rogowski, 2023). 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 operating within the Łukasiewicz-EMAG institute. Both the laboratory and the CB were to be the first entities of this type accredited by Polish Centre for Accreditation (PCA) in the field of testing and certification of the IT security of IACS components. The article presents the use case and describes the experience of launching an accredited laboratory and Certification Body (CB) for IACS components in accordance with the IEC 62443 industry standard (IEC 62443-4-2, 2019), and the methodology (CCRA CEM, 2017). The first chapter presents the assumptions and motivations for the project. The reference was made to the current situation and existing solutions, mainly in Europe. The next chapter presents the regulatory basis, materials, methods analysed on the basis of which the laboratory, processes and required documentation were developed. A justification for the selection of the main standard for product evaluation in the laboratory is provided. Later the results of the case, experience from preparing a laboratory for the evaluation of IACS components' security functions, as well as launching the certification body. The description of the first evaluation were shortly described. Finally, conclusions from the implementation of the adopted method, experience gained from the project and expected opportunities for further development are presented.

Keywords: industrial automation and control, IACS, cybersecurity, requirements, evaluation, IT security facilities

1. Introduction

For several years now, we have been observing intensified activities in Europe aimed at ensuring better ICT security standards and developing quick schemes for the assessment and certification of cybersecurity products. European initiatives (ICCS, 2020) (CSPCERT, 2019) (VARIoT, 2020-2022) and national programs and thematic projects in this area (NCBiR, 2017) (KSO3C, 2018-2022) (IŁ, 2020-2023) have been launched. In response to these activities, the Łukasiewicz-EMAG institute and NASK-PIB proposed and are implementing the CyberBEAM project (CyberBEAM, 2021-2024).

The subject of the project is to expand the cybersecurity compliance assessment and certification activities carried out by these institutions, in particular in the area of industrial components. This extension aims to develop and implement a light, faster (fixed-time) cybersecurity assessment and certification system in the field of Industrial Automation and Control Systems (IACS), Industrial Internet of Things (IIoT), Internet of Things (IoT) and Data Processing Centers/Cloud computing. Activities in the first two of the above-mentioned areas are implemented by Łukasiewicz-EMAG, while in the last two areas, activities are implemented by NASK-PIB.

Accredited Laboratory (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 IIoT, IACS, and accreditation could be extended to include an assessment in this area.

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, based on even closer cooperation and faster contact with the client submitting the product for evaluation, and in line with industry standard for security requirements IEC 62443-4-2 (IEC 62443-4-2, 2019).

For these reasons, an analysis of documentation and implementation processes of light assessment schemes implemented in European countries was carried out, i.e. CSPN in France, (ANSSI, 2023), BSZ in Germany (BSI, 2023), LINCE in Spain (CCN, 2020).

The number of existing laboratories and certification bodies certifying (in terms of cybersecurity) IT products, including IACS and IoT/IIoT, may turn out to be too small in relation to the needs that may arise with growing requirements and new EU regulations on the European market, such as the Cybersecurity Act (EU Parliament, 2019) (EU Parliament, 2022). Activities under the CyberBEAM project are intended to help reduce this problem. As a result of the project activities, analysis of existing European solutions, adaptation to the local environment, local conditions, the ITSEF laboratory operating in Łukasiewicz-EMAG obtained the first in Poland accreditation for the evaluation and certification of compliance of IACS components with the industrial standard IEC 62443-4-2 (PCA, 2022).

2. Materials and Methods

When implementing the assessment method (Rogowski, 2023) in the laboratory, experience from the implementation of the lightweight certification schemes mentioned in the previous chapter in other European countries was taken into account. Primarily LINCE, but also BSZ and CSPN.

These schemes supported mainly the development of processes for the implementation of fast evaluations of industrial components in the ITSEF laboratory, still based on own procedures developed and certified for compliance with the Common Criteria standard.

Regarding the development of a list of requirements for the evaluation of devices, the above schemes were analyzed, but also other standards, the requirements evaluated by various groups of producers and users of IACS, but also IIoT/IoT (Industrial/Internet of Things) devices were analyzed. Materials, standards, requirements. reviewed include: 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 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).

An analysis of these standards, their approach to specifying security requirements, but also a list of these security features and the way they are grouped was carried out.

When selecting the standard for extending ITSEF evaluations to IACS, IIoT and extending the Common Criteria methodology, after preselection of methods and standards, finally such selection criteria were taken into account as: the status of an international standard, similarity to the Common Criteria, ERNCIP recommendations, or knowledge and experience available in the ITSEF laboratory. More detailed information on this topic and comparison results are provided in table 4 in (Rogowski, 2023). (Leszczyna, 2018) also presents an overview of standards in the area of cybersecurity and privacy for smart grids.

All the standards touch more or less on the same groups of issues, threats and security measures as the widely used industrial standard IEC 62443 for the assessment of Industrial Automation and Control Systems and components. Hence, in determining the required actions and the list of IACS components' security requirements, the IEC 62443-4-2 standard became the basis.

Due to its familiarity, popularity and use in industry, common elements with CC standard but also a simple structure, with a specific set of functions and properties for evaluation, this standard was selected for implementation in the ITSEF evaluation practices.

3. Process and results of the pilot evaluation

3.1. Preparation of documentation for laboratory operation

The development of processes and documentation for carrying out IACS components evaluations required adapting the existing procedures of the ITSEF laboratory.

Preparation for the pilot evaluation required the development of a new testing method in the laboratory, i.e. the Security Requirements Testing Method for IACS, and its supporting annexes, such as Verification card of the

method used for evaluation, Evaluation report template for the client, Evaluation report template for the Certification Body.

The document describing the method contains technical requirements based on the IEC 62443-4-2 standard, with general tests (details depend on the specific component) and test acceptance conditions.

A very important document that was developed is so-called STIC – a template document for describing the target of the evaluation (ToE).

The document called (in the ITSEF laboratory) „STIC" (Security Target for Industrial Component) is a simplified version of the Security Target (ST) document introduced by the Common Criteria standard. The STIC task is to present the security problem in a simplified way compared to CC.

The basis for the development was mainly the following: own CC assessment documentation, Teletrust documentation, IACS Cybersecurity Certification Framework (ICCF) (Theron & Lazari, 2018), LINCE documentation.

In addition to the standard product and user documentation, the vendor of the ToE had to develop and present (based on the STIC template) also materials describing such additional elements as:

- the TOE runtime environment (e.g. operating system, external components necessary for the proper functioning of the TOE, etc.), assumptions about the operating environment that are taken into account when conducting the assessment,
- sensitive assets that the TOE must protect,
- threats that TOE must face,
- security features implemented by the TOE to counteract identified threats (similar to the security problem with CC),
- where verification of functions is not possible through normal use, it is advisable to provide evidence confirming the operation of this functions (e.g. code elements confirming their implementation, etc.).

Security problem definition according to CC and IEC 62443

In the case of the Common Criteria standard, the product vendor determines the security problem and the scope of the assessment (e.g. in ST or by declaring an assessment according to the Collaborative Protection Profile - cPP). In the case of assessment according to IEC 62443, the security problem is already largely defined by the requirements of the standard. It is clearly indicated what resources should be protected and against what types of activities. For example, system logs, depending on the security level, should be protected against loss or manipulation. Based on the requirements, a security problem can be developed for evaluation on the basis of an initial proposal (template). If this solution was chosen, the product vendor would only have to indicate how it protects the indicated resources and how it implements the indicated security functions. Completing such a document by the vendor is also an initial self-assessment of the product's readiness for certification. The vendor then independently analyzes the implementation of the required safety functions, and if the required functions are not implemented, prepares an appropriate justification, or alternatively indicates how to meet the requirements within the system in which the component is intended to work (transferring the requirement to assumptions for the environment or another system component).

A more detailed comparison of IEC and Common Criteria security target structures can be found in (Rogowski, 2023).

Taking into account the above, the description of the security problem is accomplished by placing in the STIC document two tables to be filled out (see Table 1 and Table 2 later in the article):

- Threats to critical assets – all component assets that require protection by implemented security functions or by the environment (assumptions for the environment) should be listed. It is also necessary to indicate here threats to the protected assets and threat actors (authorized and unauthorized entities) that operate on these assets.
- Security functions – all security features implemented to protect important assets must be presented. An important element of this description is information about the possibility and method of testing the correct operation of a given function, which was carried out by the vendor. Optionally, if the vendor has knowledge of the requirements of the IEC 62443 standard, it can provide a mapping of the security functions to the requirements of the standard (as the mentioned element of self-assessment of the product's readiness for evaluation).

3.2. IACS components evaluation process definition

Finally established security requirements evaluation process includes following main steps:

- Verification of the purpose of the Target of Evaluation (ToE);
- Evaluation of design documentation;
- Evaluation of user documentation;
- Examination of security requirements;

- Vulnerability analysis;
- Security requirements list selection (according to the requested Security Level);
- Evaluation of compliance with requirements:
    - Test scenarios;
    - Acceptance criteria;
    - Verdict;
    - Justification.

3.3. Evaluation process validation – IACS component evaluation

Having already defined the assessment implementation process, developed assessment method and required documentation for the implementation of evaluation activities in the laboratory, it was possible to start the implementation of the pilot evaluation of the IACS component.

The Target of Evaluation was the industrial PLC (Programmable Logic Controller) - programmable line distance protection controller for power substations provided by our partner (Figure 1).

Fig. 1. Target of Evaluation (ToE) – programmable line distance protection controller.

The vendor, together with the product, delivered documentation for evaluation, including a product short description (leaflet), user manual, communication module instruction, description of communication with the ToE, as well as a completed STIC document with the definition of the security problem and the previously mentioned key tables specifying the security problem definition:

- Threats to critical assets (Table 1) – start from the critical assets and its threat actors, to security functions.
- Security functions (Table 2) – the list of security functions with short notes and descriptions on how they can be tested.

Table 1. Threats to critical assets.

Critical asset	Threat	Actor	Security functions (see Table 5)	Environment assumption
(…)	(…)	(…)	(…)	(…)
FW – Firmware	Unauthorized change	AT, AU	F02, F04, F05, F06, F08, F09, F10, F11, F12	S01
LS – Audit records	Manipulation	AT, AU, OT	F01, F02, F08, F09, F10, F11, F12	S01
	Integrity lost	AT, AU, OT	F01, F08, F09, F10, F11, F12	S01
	Timestamp reliability	AT, AU	F04	
	Accessibility lost	AT, OT	F07	S01
(…)	(…)	(…)	(…)	(…)

Table 2. Security functions.

Security function	Description (functionality)	Testing method	CR coverage
(…)	(…)	(…)	(…)
F04 – Realiable timestamp	Remote NTP server RTC synchronization	Comparation RTC time with source after synchronization	CR 1.9 CR 2.11
F05 – Integrity check (firmware, settings)	CRC checksum	Simulation memory failure by removing module. Attempt to import corrupted file.	CR 3.14
(…)	(…)	(…)	(…)

After the TOE was delivered, installation in the laboratory and elaboration of test cases were carried out, according to the required Security Level.

A key element for both requirements preparation and minor assessment is the selection and interpretation of the security level.

For the pilot evaluation, the analysis and assessment were carried out for the SL-1 level, which defines the attacker's potential as unintentional and accidental actions not intended to lead to irregularities, disclosure or damage to a component or system. Compared to the CC standard, this potential is lower than the EAL 1 level.

The next, higher levels define an attacker who conducts deliberate actions aimed at revealing sensitive data, causing abnormal situation or causing damage to a component or system. However, for subsequent levels, the attacker's potential is defined differently and grows with it.

For the SL-2 level, the attacker's potential is assessed as low, i.e. the attacker actively searching for some vulnerabilities, but has a low level of knowledge and experience, does not have specialized equipment and does not have much motivation to achieve his goal.

For the SL-3 level, the attacker's potential is defined as moderate, where the attacker's knowledge is already at an average level in terms of knowledge of IACS systems, and he also has average equipment and motivation.

For the highest level of SL-4, the motivation level of the attacker's knowledge and resources is defined as high.

Table 33 presented in (Rogowski, 2023) includes a proposal to map SL 1 - 4 (IEC) to EAL 1 – 7 (CC), as well as to security levels (Basic, Substantial, High) defined by the Cybersecurity Act (EU Parliament, 2019). The table also takes into account the expected Attack potential values at each SL level for which ToE should be resistant.

At the moment, our considerations and work are limited to the SL-1, SL-2 and SL-3 levels, because our interest is in fast evaluation for low security levels. If an evaluation is needed for the SL-4 level, it is estimated that the cost and time will be comparable to an evaluation under CC .

Below (Table 3) is an example of an increase of requirements for the selected requirement "CR 1.1 User identification and authentication".

Table 3. An example of increasing the number of requirements as SL increases.

Requirement	SL 1	SL 2	SL 3	Verdict
FR 1				P/N/NA
CR 1.1	+	RE (1)	RE (2)	P/N/NA
(…)	(…)	(…)	(…)	(…)

Detailed description of the requirement and acceptance conditions for the CR 1.1 requirement (Human user identification and authentication) depending on the SL level.

Each level contains all the requirements from the previous one - see the table above. The Requirement Enhancement appearing at the SL-2 level (***unique*** authentication) is marked in ***italics***, while the subsequent Requirement Enhancements for the SL-3 level (***multifactor authentication***) are marked in ***italics and underlined*** font.

Example of test plan for CR 1.1 evaluation (prepared prior evaluation, is developed on the basis of an analysis of the ToE, the requirements and conditions of acceptance):

- identification of all available human users interfaces (local – the control panel of the device, network – connection through an application),
- verification of identification and authentication for each identified interface,
- analysis of potential emergency situations,
- evaluation of behavior (usage of identification) during emergency situations.

Table 4. Sample description of a single requirement in STIC and the requirement assessment summary

CR 1.1 Human user identification and authentication

The evaluator shall assess whether component provide for all interfaces with human access

- possibility of ***unique*** authentication;
- ***possibility of capability to employ multifactor authentication***

and identification and authentication:

- should not hamper fast, local emergency actions;
- should be enforced before action;
- should be in accordance with policies and roles.

Hints:

- This requirement address only interfaces with human access (such as touchscreens, buttons and also network interfaces designed for human users interaction and configuration tools) and not apply to services or software (APIs) interfaces.

Acceptance criteria • *unique* authentication of human users on all interfaces with human access • *capability to employ multifactor authentication for all human user access to the component* • identification and authentication not hamper fast, local emergency actions.	
Evaluator	
Date	
Verdict	Pass/Fail/NA

3.4. Results of the evaluation process validation

The attack potential of tests depends on SL level. During testing, the crucial thing was choosing the potential of an attack. Sometimes the tests were more strict than SL 1 (could be compared to the EAL1 level of CC standards) but even though the verdict was positive. So in some aspect the product is probably ready for higher security level than SL 1.

Possibility of exclusion of some CR requirements

Unlike a system that consists of many components, not every component will be able to meet all the requirements of the standard. The standard defines the types of components (e.g. Host/Network/Embedded Device Requirement), however a component may not meet certain requirements, e.g. due to not using appropriate technology (e.g. it is impossible to assess the requirements related to wireless networks for a component that does not have wireless interfaces). Also, part of the security-related functionality may be delegated to other components in the system or to assumptions for the environment. An example here may be the requirements for protecting the confidentiality of transmitted information, e.g. through network interfaces. The component itself may does not offer network traffic encryption, because it is intended to work in closed facilities with controlled access, e.g. control cabinet or the traffic going outside the controlled zone can be carried out using an additional component, e.g. a router with an encrypted VPN channel function. In such a case, the requirement must be met by the component's environment (in accordance with the assumptions for the environment), which, however, is not checked in the case of component evaluation. The vendor of the assessed component should declare (e.g. in the STIC document) which requirements are to be assessed and which are excluded from the assessment and for what reason. Such a declaration must also be reflected in the issued certificate, because, unlike the CC standard, we do not have a public ST document containing information on what functionality was assessed. Therefore, the potential end user should have information on the certificate about the scope of the assessment and what requirements were not assessed.

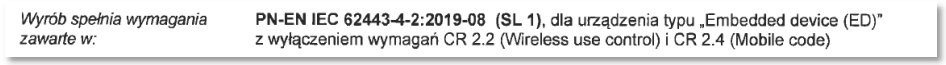

Fig. 2. Example of information included on the certificate informing about the device type (EDR) and exclusion from the assessment of CR 2.2, CR 2.4 requirements.

Reports preparation

The summary of the evaluation carried out is included in two main documents, based on Security Requirements Testing Method for IACS (M-005 internal procedure) developed in laboratory:

- The test report for the client (M-005/2 attachment) - presented to the client, containing information about the test results,
- The test report for the Certification Body (M-005/3 attachment) - transferred to the certification body for the purposes of the certification process, which includes an assessment of the product documentation and its test results, review and giving the decision on certification.

3.5. Certification Body establishment and product certification

In addition to extending the ITSEF laboratory scope of evaluation, Łukasiewicz-EMAG Institute also started work on establishing the IACS products Certification Body.

Łukasiewicz-EMAG already operates a Product Certification Body (CB), which has an implemented management system compliant with the ISO/IEC 17065 standard (ISO/IEC 17065, 2013). This management system is accredited by the Polish Accreditation Center (certificate no AC 053).

In Łukasiewicz-EMAG two certification programs are accredited:

- program CBC-1a confirming compliance with a specific normative document,
- program CBC-1b issued for samples, batches, individual products and systems.

The CBC-1a program describes the certification of electrical and electronic products with ICS codes, and after analysis of this program, its suitability for certification of IACS and IIoT products was confirmed.

Confirmation of the CB's competence to conduct certification in an extended scope (in this case, for IACS products) requires carrying out an exemplary process, which is later assessed by the Accreditation Body.

After the ITSEF laboratory obtained PCA accreditation to conduct IACS product assessments, and after conducting the first product assessment, it was possible to apply for extension of accreditation.

The report on the pilot evaluation carried out in the ITSEF laboratory was the basis for the product assessment carried out at CB. The certification process then was carried out in accordance with the IEC 62443-4-2 standard (IEC 62443-4-2, 2019).

The basic requirement for the Certification Body is to ensure impartiality during the certification processes, hence people were selected from among the ITSEF staff who did not participate in the evaluation process of the ToE and could impartially assess the evaluators' activities.

The certification process included the following stages:

- Review of the certification application,
- Carrying out an assessment of the certified product,
- Review of all documents and records,
- Making a decision and issuing a certificate.

In accordance with this process, a pilot certification was carried out and certificate of conformity No. 7494/2023 was issued.

The certification process has also been subject to an internal audit, and then the PCA audit took place, during which the competence of the unit to conduct certification in the new area was assessed. The basis for the assessment was the pilot certification process described above to the IEC 62443-4-2 standard (IEC 62443-4-2, 2019). After obtaining a positive result, PCA issued a new AC 053 certification scope for Łukasiewicz-EMAG Certification Body, extended with the IEC 62443-4-2 standard.

After obtaining accreditation, the laboratory could finally issue a certificate of compliance for the tested ToE.

4. Conclusions and observations

The validation of the method shows that (as in any assessment of this type) the key to quick, correct certification is a good definition of the scope of required documentation and the scope of information that the vendor should provide before the laboratory starts testing.

The product (ToE) vendor must be aware of the need to specify all elements of the ToE characteristics, as presented in the previous section (when presenting the results and content of STIC).

An important element is the description of assumptions regarding the environment of the ToE (both technical and procedural, because some of the security measures may be implemented by the environment), which are also taken into account during tests. When security measure is a procedure/environment, it should be indicated in the verdict so that the person reading the report is aware that the component itself, without meeting additional requirements, does not meet a given CR.

It is also important to specify in the contract the scope of participation of the vendor representative (a contact person), who will be able to quickly answer questions and doubts.

The scope of IACS equipment and the scope of required knowledge can be very wide. With such specialized equipment as IACS devices, it is important that the vendor presents a test environment that takes into account and simulates at least a part of the operating environment (at least those parts needed to test security functions related to the controlled object). Without this, an evaluators may not have the appropriate knowledge to properly configure the device for operation and better test, for example, its behavior in emergency situations, the need for recovery and the impact during normal operation.

It is important to establish at the outset a consistent approach to product assessment for each Security Level (SL) and to clarify the assessment criteria in the context of the attack potential specified in the standard. For example, for the SL-1 level, when determining tests, it should be remembered that SL-1 means low potential: commonly available knowledge, no specialist knowledge required, the attacker has commonly available equipment, applications, without deep knowledge of how to use them, etc.

During the pilot evaluation, it was also possible to develop an approach according to which the relationships between the assessed CRs were identified. When assessing CRs at a given level (e.g. SL-1), thematically related CRs that are not within the scope of a given SL but may have some impact on the assessment of that SL are taken into account. For example, when considering the security of information, event logs (CR3.4 Software and information integrity), the integrity of audit logs may also be related to some extent to the issue CR3.9 (Protection of audit information), which is no longer included into a set of requirements for the SL-1.

Sieć Badawcza Łukasiewicz
– Instytut Technik Innowacyjnych EMAG

Centrum Badań i Certyfikacji

CERTYFIKAT ZGODNOŚCI

Nr 7494/2023

Nazwa i adres dostawcy:	**Zakład Produkcyjny Aparatury Elektrycznej (ZPrAE) Sp. z o.o.,** ul. Konopnickiej 13, 41-100 Siemianowice Śląskie
Nazwa i adres producenta:	**Zakład Produkcyjny Aparatury Elektrycznej (ZPrAE) Sp. z o.o.,** ul. Konopnickiej 13, 41-100 Siemianowice Śląskie
Nazwa wyrobu:	**Terminal Zabezpieczeniowy TZX-11**
Typ (odmiany):	**TZO-11 – zabezpieczenie odległościowe, wersja oprogramowania TZO-3.3.1**
Podstawowe parametry:	Urządzenie TZO-11 z modułem komunikacyjnym MGB-9F 1/S, Oprogramowanie narzędziowe do obsługi urządzenia ZPrAE Explorer v. 2.2. Podczas użytkowania urządzenia, muszą być uwzględnione uwarunkowania bezpieczeństwa opisane w dokumentacji i instrukcji urządzenia dostarczanej przez producenta.
Wyrób spełnia wymagania zawarte w:	**PN-EN IEC 62443-4-2:2019-08 (SL 1)**, dla urządzenia typu „Embedded device (ED)" z wyłączeniem wymagań CR 2.2 (Wireless use control) i CR 2.4 (Mobile code)
Zgodnie ze sprawozdaniem z badań wykonanych przez:	**Laboratorium Oceny Bezpieczeństwa Produktów Teleinformatycznych ITSEF-EMAG** 40-189 Katowice, ul. Leopolda 31
Nr i data sprawozdania:	**2/ITSEF/2023 z dnia 21.03.2023**
Okres ważności certyfikatu:	**24.04.2023 r. ÷ 23.04.2026 r.**

Certyfikat wydany w programie certyfikacji CBC-1a

Katowice, 02.08.2023 r. Zatwierdził Tomasz Woźnica

podpis

Niniejszy certyfikat odnosi się do określonego w nim typu wyrobu i nie obejmuje nadzoru nad produkcją. Producent jest uprawniony do wydawania oświadczeń/deklaracji, że kolejne wyprodukowane egzemplarze wyrobów spełniają wyspecyfikowane wymagania.

40-189 Katowice, ul Leopolda 31 tel. +48 (32) 2007-700, fax. +48 (32) 2007-701, e-mail: cbc@emag.lukasiewicz.gov.pl, http://www.emag.lukasiewicz.gov.pl

PC–1/7 wyd. 10 z 02.08.2022 r.

Fig. 3. Certificate of the ToE compliance with IEC 62443-4-2.

Cross-check

Since the aim of the work was to obtain accreditation, the quality of the work had to be ensured. For this purpose, a cross-check system was introduced – evaluation of one evaluator's work by another. The system was used both during analytical work (preparation of requirements and acceptance conditions) and during the pilot evaluation itself, and the entire process was documented for the purposes of the accreditation audit.

Supplemental guidance

An additional element developed during the analysis of the standard and the preparation of requirements was supplemental guidance. They were created based on the analysis of the standard, similar assessment schemes and evaluators' experiences during Common Criteria evaluations. Their task is to clarify the standard's requirements and to indicate critical aspects of the evaluation.

5. Summary

Goal of the CyberBEAM project is to build fast cybersecurity certification programs for IoT, IIoT, Data Centres, Cloud Computing and IACS devices.

The documents, process developed and the experience gained during this work are planned to be used for extending the accreditation to higher security levels (SL-2 and SL-3), and for developing and implementing lightweight assessment schemes of industrial automation and control systems components' in Poland.

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) 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. 2020. Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE). Guía de Seguridad de las TIC, Issue CCN-STIC 2002.

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

CSPCERT. 2019. European Cloud Service Provider Certification (CSPCERT) Working Group. Available at: https://www.cspcert.eu/ [Accessed 28 12 2023].

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].

EU Parliament. 2019. Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communication technology cybersecurity certification and repealing Regulation (EU) No 526/2013, s.l.: Official Journal of the European Union.

EU Parliament. 2022. Directive (EU) 2022/2555 of the EU Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.

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).

ICCS. 2020. IACS Components Cybersecurity Certification Scheme. Available at: https://erncip-project.jrc.ec.europa.eu/networks/tgs/european-iacs [Accessed 28 12 2023].

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].

IŁ. 2020-2023. Eksperymentalna Platforma Walidacyjna. Available at: https://www.gov.pl/web/instytut-lacznosci/epw [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.

ISO/IEC 17065. 2013. Ocena zgodności - Wymagania dla jednostek certyfikujących wyroby, procesy i usługi (Conformity assessment - Requirements for bodies certifying products, processes and services).

JRC. 2020. Recommendations for the implementation of the Industrial Automation & Control Systems Components Cybersecurity Certification Scheme (ICCS). ERNCIP Thematic Group: IACS Cybersecurity Certification Framework (ICCF).

KSO3C. 2018-2022. Krajowy schemat oceny i certyfikacji bezpieczeństwa oraz prywatności produktów i systemów IT zgodny z Common Criteria. Available at: https://www.kso3c.pl/ [Accessed 28 12 2023].

Leszczyna, R. 2018. Cybersecurity and privacy in standards for smart grids – A comprehensive survey, Volume 56, pp. 62-73.

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

NCBiR. 2017. CyberSecIdent - Cyberbezpieczeństwo i e-Tożsamość. Available at: https://archiwum.ncbr.gov.pl/programy/programy-krajowe/cybersecident/

PCA. 2022. Scope of accreditation for testing laboratory, No AB 1781. Polskie Centrum Akredytacji.

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.

Theron, P. & Lazari, A. 2018. The IACS Cybersecurity Certification Framework (ICCF). Lessons from the 2017 study of the state of the art. EUR 29237 EN, Luxembourg: Publications Office of the European Union.

VARIoT 2020-2022. Vulnerability and Attack Repository for IoT. Available at: https://www.variot.eu/ [Accessed 28 12 2023].