Advances in Reliability, Safety and Security, Part 7 – Kołowrocki, Magryta-Mut (eds.)

Advances in Reliability, Safety and Security

ESREL 2024
Monograph Book Series

How To Apply Common Criteria Methodology To IACS Components Security

Dariusz Rogowski, Artur Kozłowski

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

Abstract

Industrial Automation and Control Systems (IACS) and their components are currently becoming increasingly a target of cyberattacks. This is why the industry applies different security measures to protect IACS' critical assets. The question is whether these measures are efficient and reliable enough to counter cyberthreats? The security evaluation methodology for the IACS components would help answering this question. But currently there is no such a methodology intended for industrial devices. In the paper, we propose to apply the Common Criteria (CC) standard (ISO/IEC 15408) and the Common Evaluation Methodology CEM (ISO/IEC 18045) to the IACS components security evaluation. Hence the Common Criteria is dedicated to Information Technology (IT) products it must be adapted to the security requirements of industrial products. The paper describes how the CC and CEM methodologies were supplemented and adjusted to qualities and requirements specific to the industrial components. The adaptation was based on the IEC 62443 family of standards which include industrial technical security requirements. The CC-based methodology for IACS was validated by the IT Security Evaluation Facility (ITSEF) located in Łukasiewicz – EMAG Institute. The methodology was applied to the security evaluation of a programmable logic controller. The evaluation results confirmed the methodology can be used for the security evaluation of industrial devices.

Keywords: common criteria, security requirements, security evaluation, industrial automation and control system

1. Introduction

Industrial automation control networks (Operation Technology, OT) are often integrated with enterprise IT networks which are connected to the Internet. It allows remote monitoring and management of industrial systems but at the same time it exposes them to threats and attacks typical for IT solutions. This is why entrepreneurs apply security measures to counter IT threats. But the security measures can be of different quality and efficiency that lead to the following question: how to assess these qualities and how to gain more assurance to industrial security controls?

The answer lays in the security evaluation process run by an independent, accredited laboratory which implements standards describing security requirements and evaluation methodologies. Such a laboratory, called the IT Security Evaluation Facility (ITSEF), was established in Łukasiewicz – EMAG Institute (ITSEF-EMAG, 2024).

ITSEF was built in the result of a R&D project "National schema for the security and privacy evaluation and certification of IT products and systems compliant with Common Criteria (KSO3C)", 2018 – 2022 (KSO3C, 2022). In 2021 ITSEF received the accreditation of the Polish Center for Accreditation (PCA) in accordance with the requirements of ISO/IEC 17025 – certificate no AB 1781 (PCA, 2024). The accreditation confirms ITSEF has got technical capabilities and expertise to carry out security evaluations in accordance with the Common Criteria.

In 2022 the Polish evaluation and certification scheme changed its status to authorized within two international arrangements: SOG-IS – Mutual Recognition Agreement of Information Technology Security Evaluation Certificates (SOG-IS, 2010) and CCRA – Arrangement on the Recognition of Common Criteria Certificates (CCRA, 2014). Security certificates are mutually recognized by all the signatories of both arrangements.

In 2022 the ITSEF laboratory extended its scope of accreditation to the security evaluation of industrial devices in accordance with the IEC 62443-4-2 standard (IEC-62443-4-2, 2019). The new scope was the result of a

successful pilot security evaluation of industrial programmable controller carried out by ITSEF. The main goal of that evaluation was to validate an evaluation methodology for IACS devices created in another R&D project "Cybersecurity evaluation and certification – smart certification schemes (CyberBEAM)", (Grant No. CYBERSECIDENT/ 489595/ IV/ NCBR/ 2021), 2021 – 2024. The pilot evaluation results were also used in the validation of CC-based methodology for IACS presented in this paper as well as in a doctoral thesis (Rogowski, 2023).

The CyberBEAM project goal is to develop the so-called lightweight, in terms of short execution time and lower costs, cybersecurity evaluation and certification scheme for IACS devices. The IACS certification scheme will be complementary to the Common Criteria certification scheme developed in the KSO3C project. Additionally, the scheme will meet the guidelines of future EU cybersecurity certification schemes what will be presented later in this paper. Therefore, using a combination of IT and industrial security requirements seems to be a promising approach in the development of security certification schemes dedicated to the new types of products.

Currently there are many standards which describe industrial security requirements and evaluation criteria. But none of them includes evaluation methodologies explaining how to use these criteria during the evaluation. What is more they do not use so called Evaluation Assurance Levels (EAL) which are used for IT products.

The EAL is the one of basic terms in the Common Criteria for Information Technology Security Evaluation standard (CC, 2022). Common Criteria is also described in the international standard ISO/IEC 15408 (ISO_15408, 2022). Additionally, the CC is supplemented by the Common Evaluation Methodology, CEM (CEM, 2022) which is described in the international standard ISO/IEC 18045 (ISO_18045, 2022). In the CEM, assurance of security evaluation is measured by EAL, which defines the rigor and details of the evaluation process and says how much trustful and reliable is the security evaluation of an IT product. There are seven levels of assurance: EAL 1 to EAL 7. The higher EAL the more detailed and stringent security requirements are used for testing the security functionality of a product and for verifying its technical and guidance documentation.

So far, according to CC (CC_Portal, 2024), there have been certified more than 5600 different types of IT products such as: integrated circuits (IC) and smart cards, firewalls, operating systems, data bases, products for digital signatures, access control devices and systems (ex. Biometric sensors) (Białas, 2019), intelligent sensors (Białas, 2016), and many others. No products from the field of industrial automation have been evaluated in accordance with CC.

The reason is that CC methodology does not include requirements and criteria intended for the industry solutions. But is it possible to adapt the CC in such a way that it could meet the industrial security requirements? And if so, could it be then used for the security evaluation of industrial devices? In the paper the authors answer these questions.

The paper is organized as follows. Section 2 presents the research problem and state of the art in the field of IACS cybersecurity methodologies and standards. The chapter describes Common Criteria methodology and the results of European Union research in the field of security certification. Section 3 summarizes the adaptation of the Common Criteria standard to industrial security requirements and shows the model of CC-based evaluation process for IACS. Section 4 presents the CC-based evaluation methodology and the results of its validation, and section 5 presents conclusions and future works.

2. Research problem and state of the art

The research problem results from the lack of a security evaluation methodology intended for IACS devices. In the context of cybersecurity certification for industrial solutions, the research results of The European Reference Network for Critical Infrastructure Protection Thematic Group (ERNCIP TG) are very interesting and worth to mention (Theron & Bologna, 2014). The group started to operate in 2014 and since then it elaborated guidelines for setting up the European cybersecurity certification framework dedicated to IACS called IACS Cybersecurity Certification Framework – ICCF (Theron & Lazari, 2018). Next, in 2020, the group worked out and published recommendations for the implementation of IACS Certification Schemes (ICCS), (Theron, et al., 2020). The recommendations are in accordance with Cyber Security Act (CSA) provisions (EU_Parliament, 2019) so that they can be applied by Certification Bodies (CB), Conformity Assessment Bodies (CAB), and security evaluation laboratories like Common Criteria conformant ITSEFs (IT Security Evaluation Facility).

What is more, The European Union Agency for Cybersecurity (ENISA) promotes Common Criteria as a prospective methodology for security certification. Hence, in 2021 ENISA proposed the draft candidate of EU Cybersecurity Certification Scheme (EUCC) based on Common Criteria and conformant with SOG-IS MRA (Senior Officials Group - Information Systems Security Mutual Recognition Agreement) (SOG-IS, 2010), (SOG-IS_Portal, 2024). The EUCC was finally published on February 2024 at the Official Journal of the European Union

in Regulation (EU) 2024/482 (EUR-Lex, 2024). The regulation lays down the rules for the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

The ERNCIP TG pointed out the lack of harmonized security evaluation methodologies for IACS devices. The group also suggested the development of evaluation methodologies for IACS with a maximum reuse of existing methodologies like Common Criteria and the industrial security requirements included e.g. in the IEC 62443 series of standards (established by the International Society of Automation, ISA) (ISA, 2024).

In the past in some publications like (Xie, et al., 2014), (Colbert & Kott, 2016), (Leszczyna, 2018), (Rogowski, 2018) the authors found out the CC had some capabilities to be used for IACS products. But the CC standard still is not used for industrial devices even though the ENISA and ERNCIP research groups currently point out that CC could be used for that purpose. Therefore, the solution proposed in the article, – the CC-based evaluation methodology for IACS, hereinafter referred to as ICEM (IACS Common Evaluation Methodology) – is an important novelty in the field of security evaluation.

The next section briefly describes the basics of the CC standard. It also presents a short analysis whether the CC and CEM methodologies have the potential to be adapted and applied to the IACS-type of products.

2.1. Common Criteria – a short manual

According to the CC standard, the term of security assurance defines the source of trust to IT product as a rigorous and controlled process of its development, documentation, manufacture, testing, and delivery, maintained throughout the whole product's life cycle. This is to ensure that the security measures applied in the IT product are correct and sufficient to minimize the impact of the cyberthreats to critical assets (Białas, 2008). In CC terminology, IT products are referred to as Target of Evaluation (TOE). The confidence to the security measures of TOE is confirmed during an independent security evaluation process conducted by an accredited and licensed laboratory which uses the CC and CEM methodologies.

The most important are the first three parts of the CC standard. The first part, hereinafter referred to as CC p.1 (CC_p1, 2022), contains an introduction, a general assurance model, and basic terms and definitions. CC p.1 also describes the structures of documents like Security Target (ST) and Protection Profile (PP). The ST contains the specification of security functions for a specific implementation of TOE. The PP, on the other hand, contains a set of security requirements for a given type or family of IT products, not related to a specific implementation of TOE.

The second part, hereinafter referred to as CC p.2 (CC_p2, 2022), includes Security Functional Requirements (SFR) which are used to design TOE security functions (TSFs).

The third part, hereinafter referred to as CC p.3 (CC_p3, 2022), contains Security Assurance Requirements (SAR) which provide a necessary confidence for the TOE security evaluation. SARs are grouped in assurance packages called Evaluation Assurance Levels (EALs). The developers use EALs to declare the intended level of assurance to TOE security functions (Rogowski, 2014).

The EALs include the chosen subset of SAR requirements for the evaluation of: ST document, PP document, TOE guidance documentation (AGD), development documentation (ADV), life-cycle support (ALC), tests (ATE) and vulnerability assessment (AVA) (Rogowski, 2013).

The CC standard is supplemented by the CEM methodology which introduces a term of Work Unit (WU). WU is a synonym of elementary activity performed by an evaluator to issue a verdict on whether the given SAR requirement is met by the TOE or its documentation. There are three possible verdicts: 1) positive (Pass) for a met requirement; 2) negative (Fail) for an unmet requirement, and 3) inconclusive (Incl) for situations where evidence is insufficient to issue an unambiguous verdict for a requirement.

For each verdict, the evaluator must provide a rationale which includes evidence that a given requirement from EAL's package is met. The evidence can be the results of functional tests and penetration tests, the results of verification of TOE documentation, the audit results of the TOE development environment. The positive results of all SARs on the given EAL lead to the final positive evaluation of the TOE. The ITSEF's evaluation results are next validated by the Certification Body during a TOE certification process. If the validation is positive, then the TOE gets the CC security certificate for the given EAL which is published on CB's website and on the Common Criteria certified products list (CC_Portal, 2024).

The CC standard defines the SFRs and SARs requirements in the form of components. The components consist of the following obligatory content: a component's identification name and description, dependencies to other components, and the wording of a requirement. The SARs components additionally include the descriptions of activities that shall be performed by the evaluator to confirm that the requirement has been met.

The components may be used by the ST authors (TOE developers) exactly as defined in the CC p.2 and CC p.3, or they may be tailored with some operations permitted by the CC standard. This gives some flexibility to adjust SFRs and SARs in a way they can meet the TOE security objectives declared by the developer in the ST document. The permitted operations include (ISO_15446, 2009): 1) iteration – it allows a component to be used more than

once with varying operations or requirements; 2) assignment – it allows the specification of parameters; 3) selection – it allows the specification of one or more items from a list; 4) refinement – it allows the addition of details to the requirement.

In specific cases, when the author of a ST may not be able to correctly specify or refine existing components from the CC standard, the CC allows the definition of new components which are called extended components. It takes place when there are security objectives for the TOE that cannot be translated to the CC part 2 (SFRs), or there are third party requirements (e.g., standards, laws, or specific security needs for IACS devices) that cannot be translated to the CC part 3 (SARs). In both cases the ST author is required to define his own components (the extended components).

The CC standard provides some guidance for the specification of extended components which must be followed by the author of a ST. When defining extended requirements, the CC requires that they are defined in the same way as existing components in the standard. Additionally, for an extended assurance component the CC requires the definition of extended Work Units (WUs) for the evaluation methodology CEM. WUs include the activities an evaluator must perform to verify that a TOE conforms to that extended assurance component.

To summarize, despite very strict rules of using security requirement components, the standard leaves some capabilities to adapt the requirements to specific products or technologies by permitted operations or extended components. This quality of the CC was used to modify and create new components to adapt the CC methodology to the specific security needs of IACS devices.

The next chapter identifies the sources of industrial security requirements, which will constitute input data for the development of modified or extended CC requirements.

2.2. Industrial security requirements for vulnerabilities mitigation

The critical analysis of literature was used to determine the security requirements for IACS components. There were examined the standards and methods which included the recommendations of security measures to reduce the IT vulnerabilities of industrial devices. The goal of the analysis was to determine which one of the identified standards could be the input for the development of the IACS Common Evaluation Methodology (ICEM) and adaptation of CC requirements.

Many reports about the IT vulnerabilities of industrial systems made by such institutions as CyberX (CyberX, 2017) or ICS-CERT (Industrial Control Systems – Cyber Emergency Response Team) (ICS_CERT, 2023) show an increasing number of identified vulnerabilities. For example, ICS-CERT pointed out the following top six weakness categories in order of prevalence (ICS-CERT, 2016):

- Boundary protection – weaker boundaries between OT networks and enterprise networks can cause undetected unauthorized activity in critical IACS system.
- Least functionality – additional, unnecessary functions in a device can increase the risk of an extended attack vector for malicious party access to critical assets.
- Identification and authentication – extended risk caused by the lack of accountability and traceability for user actions if an account is compromised, or by increased difficulty in securing accounts as personnel leave the organization.
- Physical access control – an unauthorized physical access to field equipment and locations provides increased opportunity to: maliciously modify, delete, or copy device programs and firmware; access to OT networks; steal or vandalize cyber assets; add rouge devices to capture and retransmit network traffic.
- Audit review, analysis, and reporting – without formalized review and validation of logs, unauthorized users, applications, or other, unauthorized events may be present in the system and operate without detection.
- Authenticator management – compromised unsecured password communications could allow attackers listen to the traffic and intercept credentials. If a password is compromised, the system assumes the user is an authorized party and gives a persistent access to the system.

There are many security recommendations published in standards, special publications, or guidelines (Piggin, 2013), (Zhou, et al., 2017), (Leszczyna, 2018) which can be used to mitigate the risk of vulnerabilities exploitation. The examples of most known publications are the following:

- IEC 62443 – the family of standards which includes requirements for improving the safety, availability, integrity and confidentiality of components or systems for industrial automation and control. The family of standards includes elements arranged in four groups, corresponding to the primary focus, and intended audience: 1) General; 2) Policies and procedures; 3) System; 4) Component. The fourth group includes specific and detailed requirements associated with the development of IACS products:
    - IEC 62443-4-1 (IEC-62443-4-1, 2018) – the standard describes the requirements that are applicable to the secure product development lifecycle.

    - IEC 62443-4-2 (IEC-62443-4-2, 2019) – the standard provides detailed technical security requirements for IACS components (Component Requirements, CRs).
- IEEE 1686 (IEEE-1686, 2023) – the standard defines the functions and features to be provided in intelligent electronic devices (IEDs) to accommodate cybersecurity programs. The standard addresses security regarding the access, operation, configuration, firmware revision and data retrieval.
- SP 800-82 – NIST (Stouffer, et al., 2015) – Guide to Industrial Control Systems (ICS) Security which provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

The ERNCIP Thematic Group pointed out the IEC 62443 standard was applied in the proprietary ISA Secure Certification Program (Theron & Bologna, 2014) called EDSA (Embedded Device Secure Assurance). The same group indicated the TeleTrust lightweight security evaluation methodology for industrial devices (Fritsch, et al., 2019) which follows the IEC 62443-4-1 and IEC 62443-4-2 standards. Taking above into consideration, the IEC 62443 family of standards seemed to be the primary source of requirements chosen for industrial applications.

For the final confirmation whether the IEC 62443 could be the input for the adaptation of CC security requirements we adopted the following assessment criteria:

- ISO/IEC/IEEE – it means that the document has the status of an international standard.
- IT security – it means that the requirements concern IT security issues.
- CC – it means that the requirements definition structure is like SFR and SAR components structure in the CC standard.
- ERNCIP – it means that the ERNCIP research group recommends the given solution of using IEC 62443.
- ITSEF – it means that the ITSEF Łukasiewicz – EMAG laboratory already has knowledge and experience in applying the given solution.

Table 1 presents the results of documents assessment according to the given criteria. An "X" mark means that the given document meets the criterium in the column.

Table 1. Evaluation of industrial security requirements documents.

Document / Criteria	ISO/IEC/IEEE	IT security	CC	ERNCIP	ITSEF
IEC 62443	X	X	X	X	X
NIST SP 800-82	–	X	–	X	–
IEEE 1686	X	X	–	–	–
EDSA	–	X	–	X	–
TeleTrust	–	X	X	X	X

Considering the arguments cited in publications and the results presented in Table 1, the IEC 62443-4-1 and IEC 62443-4-2 standards are the best sources of industrial requirements for the next stages of research. It is also beneficial that, as part of the CyberBEAM project, the ITSEF laboratory has gained knowledge and experience in the application of the IEC 62443 standard. Moreover, an additional argument in favor of the selected standards may be their structural similarity to the Common Criteria methodology, which will be demonstrated later in the chapter with the comparison of CC and IEC 62443 requirements.

The IEC 62443-4-1 standard contains requirements to produce a secure IACS product throughout its life cycle. Requirements for the industrial product development are summarized in eight following practices: Practice 1 – Security management, SM; Practice 2 – Specification of security requirements, SR; Practice 3 – Security by design, SD; Practice 4 – Secure implementation, SI; Practice 5 – Security verification and validation testing, SVV; Practice 6 – Management of security-related issues, DM; Practice 7 – Security update management, SUM; Practice 8 – Security guidelines, SG. These practices specify a similar scope of requirements to the ALC (Life-cycle support) class in the CC standard, what will be used for adapting SAR requirements to the practices.

The IEC 62443-4-2 standard defines the following seven technical Foundational Requirements (FRs): FR 1 – Identification and Authentication Control, IAC; FR 2 – Use Control, UC; FR 3 – System Integrity, SI; FR 4 – Data Confidentiality, DC; FR 5 – Restricted Data Flow, RDF; FR 6 – Timely Response to Events, TRE; FR 7 – Resource Availability, RA. These FRs specify a similar scope of requirements to SFRs in CC p. 2 standard, what will be used for adapting SFR requirements to FRs.

Each FR requirement contains the sets of IACS component requirements (CR). CRs may contain Requirement Enhancements (REs) that contain additional requirements to the base CR and are required at higher Security Levels (SLs). The SL means that a particular IACS component is capable of being configured to protect against an increasingly complex type of threat. In a great short, the IEC 62443 defines four security levels from SL 1 to SL 4, each with the increasing rigor of requirements. The descriptions of the SLs use terms like casual or coincidental

(SL 1), simple (SL 2), sophisticated (SL 3), and extended (SL 4) means used by an attacker to violate the security requirements of an IACS component.

The next chapter presents the adaptation methodology of Common Criteria requirements to the needs of industrial devices.

3. Methodology of CC adaptation to IACS security requirements

The chapter presents the results of the CC adaptation in the form of sets of requirements that will be used in the IACS common evaluation methodology (ICEM). The methods of comparison and critical analysis were used to discover relationships between both standards CC and IEC 62443. Next, the detailed analysis of components structure was made. Then, the component structures from both standards were synthesized into the new modified CC requirements and CEM work units.

3.1. Comparison of CC and industrial security standards

The comparison of the IEC 62443-4-1 and IEC 62443-4-2 with CC p.2 and CC p.3 respectively was made based on the following factors: 1) Security requirements – determines whether the standard has got sets of formalized requirements for both security functionality and security evaluation; 2) Testing requirements – determines whether the standard defines the requirements for testing of security functions; 3) Vulnerability analysis requirements – determines whether the standard includes requirements for vulnerability assessment.

The comparison showed the standards present similar requirements structures for the development and evaluation of security measures. This is why the following improvement directions were defined:

- CC p.3 – SARs will be adapted to Practices of IEC 62443-4-1 in the following scope: 1) SARs modifications will be based on Practices 1 – 8; 2) ATE class (Testing) modifications will be based on Practice 5.
- CC p.2 – SFRs will be adapted to FRs of IEC 62443-4-2.
- CEM – WUs will be modified or new WUs will be developed for the modified or extended SARs.
- Evaluation activities will be developed for the extended SFRs.

The adapted elements of CC and CEM were included in the model of evaluation depicted in Figure 1.

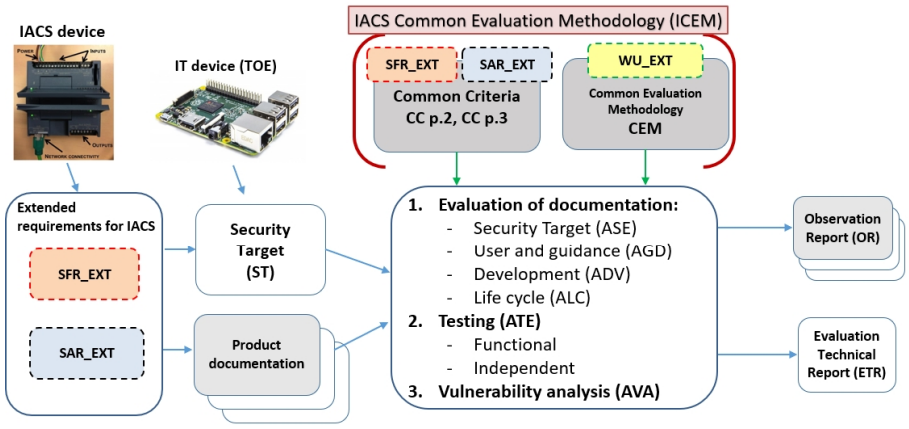

Fig. 1. Model of the CC evaluation process supplemented with extended requirements for IACS.

Figure 1 presents three main steps of CC methodology which includes the evaluation of TOE documentation, testing activities and vulnerabilities analysis. The CC standard is supplemented with the extended (or modified) requirements (elements with the EXT suffix) adapted to the industrial standard IEC 62443. In this way Common Evaluation Methodology (CEM) is adapted to be used for IACS devices. The outputs of the evaluation process are the Observation Report (OR) and Evaluation Technical Report (ETR). The OR is written by the evaluator requesting a clarification or identifying a problem during the evaluation. The ETR provides the overall verdict of an evaluation and its justification. The ETR is submitted to the Certification Body for validation.

Next section presents the way of adapting the SFR and SAR requirements from the CC p.2 and p.3 standards to the IACS security requirements.

3.2. Adaptation of Common Criteria requirements

Analysis and logical construction method, with the support of the comparison method, were used to create modified CC requirements. In the first stage the mapping of standards was made to determine pairs of related requirements for the comparison. During the comparison stage the content of requirements was analyzed to identify features specific to IACS. Next, the industry-characteristic features were applied to modify CC original requirements.

The process of creating modified and extended CC requirements was the same for both SARs and SFRs components as well as for industrial requirements. The process has the following seven steps:

1. Analysis of the structure of the industrial requirements: CRs and Practices.
2. Analysis of the structure of the SFRs and SARs components.
3. Preliminary mapping of CRs to SFRs and Practices to SARs respectively.
4. Comparison of related industrial (CR, Practice) and CC components (SFR, SAR):
    a. Selection of industrial requirement CR/ Practice.
    b. Determining an output SFR/ SAR component.
    c. Determining the comparison factor – specific industrial requirement or security feature.
    d. Identification of an industrial feature to be included in a modified or extended SFR/ SAR.
5. Combination of SFR/ SAR and the identified industrial feature into the one of following forms:
    a. Original SFR/ SAR – the content of SFR/ SAR component is unchanged because it is mapped to the CR/ Practice which fully overlap the same security requirements. In other words, original CC component's content also meets the characteristics of industrial security.
    b. SFR [*refinement, assignment*] – a component adapted with a refinement or assignment operation when the content of CC and industrial requirements partially overlap.
    c. SAR [*refinement*] – a component adapted with a refinement operation when the content of CC and industrial requirements partially overlap.
    d. SFR_EXT/ SAR_EXT – an extended component in case the industrial requirement does not have an equivalent of CC component, or an existing CC component cannot be modified by a refinement or assignment operation.
6. Development of evaluation activities for all mapped, modified, or extended SFR/ SAR components:
    a. Evaluation Activities (EAs) for SFRs which include test plans for the original CRs.
    b. Work Units (WUs) for SARs to be included in CEM.
7. Development of resulting mapping tables of CC components and industrial requirements.

The mapping tables were created which contain modified and extended CC requirements (with the EXT suffix):

- Mapping tables with SAR_EXT, WU_EXT based on the IEC 62443-4-1 standard.
- Mapping tables with SFR_EXT and EAs based on the IEC 62443-4-2 standard.

In the result of analysis of 47 Practices, 75 CRs, 24 SARs, and 32 SFRs there were created the sets of 31 SARs_EXT, 30 WUs_EXT, and 20 SFRs_EXT. These sets of requirements and Work Units were placed in the mapping tables. The detailed content of requirements and all mapping tables can be found in the doctoral thesis (Rogowski, 2023).

The integration of all CC and CEM elements adapted to IACS requirements allowed to develop the IACS Common Evaluation Methodology (ICEM) which main steps are described in the next chapter.

4. IACS Common Evaluation Methodology (ICEM)

The ICEM covers all security requirements of the Common Criteria and industrial standard. The evaluation methodology for IACS enables security evaluation thanks to modified and extended components as well as the original, unchanged SFR and SAR components.

The ICEM includes the following three main steps:

- Documentation evaluation – it includes WUs for ASE, AGD, ADV, ALC assurance classes.
- Functional and independent testing – it includes WUs for ATE assurance class.
- Vulnerability analysis – it includes WUs for AVA assurance class.

The next section presents the examples of new extended Work Units for the evaluation steps.

4.1. ICEM steps

The ICEM steps 1 and 2 with the CC part 3 requirements and extended WUs for CEM are presented on Figure 2.

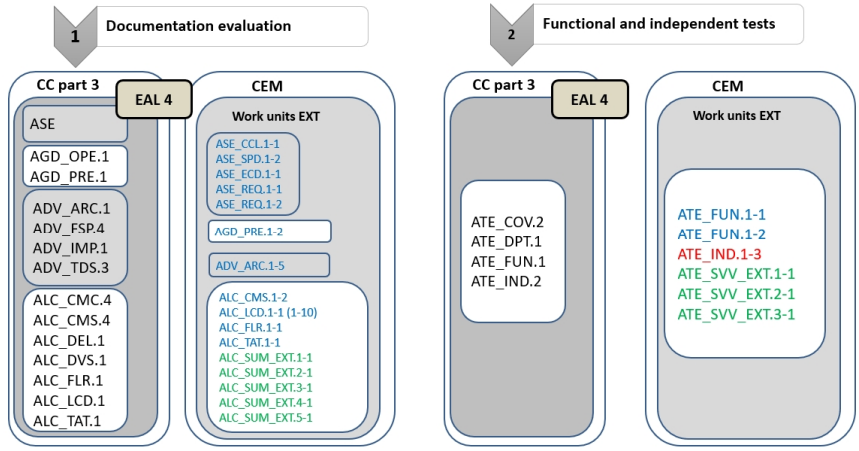

Fig. 2. The ICEM methodology with extended Work Units (WU_EXT) adapted to IACS evaluation.

Step 1 (Documentation evaluation) allows to evaluate the Security Target document, operational user guidance and preparative documentation, design and technical documentation, and life-cycle documentation. In the left frame "CC part 3" there is an example list of CC requirements for EAL 4 assurance package, while in the right frame "CEM" there are WUs_EXT adapted to IACS devices. It means that step 1 is performed with the original SARs from CC part 3 and additional WUs_EXT defined for CEM. The WUs modified with refinement operations are marked in blue, while new extended WUs are marked in green.

Step 2 (Functional and independent tests) allows to run TOE functional and independent tests according to original CC SARs and additional extended WUs (CEM) – Figure 2 presents the requirements for EAL 4. The Work Unit ATE_IND.1-3 marked in red indicates the evaluator's activities for testing TOE security functions. These activities include: the development of test plan, defining the acceptance criteria of results and defining the expected tests results. Evaluation activities defined in ATE_IND.1-3 were used during the pilot evaluation in ITSEF laboratory as a part of the ICEM validation.

Step 3 (Vulnerability analysis) is conducted fully in accordance with the AVA class defined in CC part 3 and CEM. Hence, Step 3 does not use any modified or additional SARs or WUs and this is why they are not presented on Figure 2. The main objective of the vulnerability analysis is to determine whether the potential vulnerabilities identified during the evaluation of the TOE's design process and operating environment could allow attackers to exploit vulnerabilities and violate SFRs.

4.2. ICEM validation

The details of ICEM validation were presented in the doctoral thesis (Rogowski, 2023) and the paper "First experiences in the cybersecurity evaluation and certification of IACS components" by Jacek Baginski and Rafal Kurianowicz which is going to be published in ESREL 2024 conference proceedings.

The validation was carried out by verifying all extended WUs and conducting the pilot evaluation of the programmable distance protection controller in the ITSEF laboratory. The validation embraced the following steps:

- Step 1 validation (documentation evaluation) – the verification of WUs_EXT for SAR classes ASE, AGD, ADV, ALC. It was verified whether the WUs are designed in a way that allows to assign a verdict to the given SAR requirement.
- Step 2 validation (functional and independent tests), the pilot evaluation of a programmable controller – ATE_IND.1-3 Work Unit was verified whether it can be used for the evaluation of ATE_IND.1 SAR component intended for TOE independent testing. The ITSEF tested the IACS device in accordance with the IEC 62443-4-2 standard at SL 1 level. The tests were performed for 50 industrial CRs (Component Requirements). The tests results allowed to assign a final verdict for the ATE_IND.1 component.
- Step 3 validation (vulnerability analysis) – this step was not validated because it is fully conformant with Annex B of CEM.

The results of the validation can be summarized as follows:

- Verification of the extended WU_EXT confirmed that verdicts can be issued for all SAR_EXT components.
- It is possible to issue a verdict for the ATE_IND.1 (the independent tests of TOE security functions).
- It is possible to test the TOE security functions according to modified ATE_IND.1-3 Work Unit.

In the result, the ICEM methodology provides a universal and common tool to increase the security assurance of IT and industrial products in conformity with EALs and SLs. This chapter presented three main steps of ICEM which were validated. The aim of the validation was to confirm that the methodology is suitable for the security evaluation of IACS devices.

5. Conclusions and future works

In the paper the ICEM methodology for security evaluation of IACS components was presented. The ICEM adopts the Common Criteria security assurance to the evaluations of IACS devices. It integrates IT and industrial security requirements into one evaluation methodology which strengthen the protection of IACS devices against IT as well as industrial cyber threats.

The ICEM was implemented in the ITSEF laboratory to run the pilot evaluation of industrial product in accordance with the requirements of the IEC 62443-4-2. The methodology was validated during the pilot evaluation. In the result it was confirmed that ICEM can be applied to IACS devices and the ITSEF finally extended its scope of accreditation for a new type of devices.

Future works will be focused on extending the solution based on the CC part 4 (CC_p4, 2022). The CC part 4 describes the framework for the specification of evaluation methods and activities for different types of products or specific technologies. The modified and extended CC requirements and WUs of ICEM methodology can be used for the development of evaluation methods for new types of devices, for instance for Industrial IoT (IIoT) based on CC part 4.

The other works will be focused on the development of Protection Profiles (PPs) for the given industrial devices, e.g. Programmable Logic Controllers (PLC). The PP can facilitate the development and evaluation of security measures of IACS components. The PP document will contain ready-to-implement sets of security requirements, and evaluators will receive ready-to-use sets of evaluation activities to verify these requirements.

The research results will be used for the extension of the lightweight evaluation and certification scheme developed in the CyberBEAM project.

Acknowledgments

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). The paper also draws upon the results of Dariusz Rogowski’s PhD thesis “Security evaluation method of industrial network components on the example of programmable logic controllers” (Rogowski, 2023).

References

Białas, A. 2008. Semiformal Common Criteria Compliant IT Security Development Framework, Studia Informatica vol. 29, Number 2B(77). Gliwice, Silesian University of Technology Press.

Białas, A. 2016. Computer-Aided Sensor Development Focused on Security Issues. Sensors 16.6: 759.

Białas, A. 2019. Computer Support for Development of Biometric Systems with Claimed Assurance. W: Studia Informatica, Volume 40, Number 1 (138). Gliwice: Silesian University of Technology Press, pp. 5-30.

CC_p1. 2022. Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Rev. 1, CCRA.

CC_p2. 2022. Common Criteria for Information Technology Security Evaluation. Part 2: Security functional components. Rev. 1, CCRA.

CC_p3. 2022. Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance components. Rev. 1, CCRA.

CC_p4. 2022. Common Criteria for Information Technology Security Evaluation. Part 4: Framework for the specification of evaluation methods and activities. Rev. 1, CCRA.

CC_Portal. 2024. Common Criteira Certified Products List - Statistics. [Online], Available at: https://www.commoncriteriaportal.org/products/stats/ [Date of access: 2024].

CC. 2022. Common Criteria for Information Technology Security Evaluation; Parts 1 through 5. Rev. 1, Common Criteria Management Board (CCMB).

CCRA. 2014. Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, July 2, 2014. [Online] Available at: https://www.commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.pdf [Date of access: 2024].
CEM. 2022. Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, Revision 1, Common Criteria Management Board (CCMB).
Colbert, Edward J. M., Kott, A. 2016. Cyber-security of SCADA and Ohter Industrial Control Systems. Advances in Information Security Volume 66. Fairfax, USA. Springer.
CyberX. 2017. Global ICS & IIoT Risk Report. A data-driven analysis of vulnerabilities in our critical industrial infrastructure, CyberX.
EU_Parliament, T. C. 2019. REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybesecurity Act), Brussels: Official Journal of the European Union.
EUR-Lex. 2024. Commission Implementing Regulation (EU) 2024/482 of 31 January 2024. [Online] Available at: https://eur-lex.europa.eu/eli/reg_impl/2024/482/oj [Date of access: February 2024].
Fritsch, S., 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).
ICS_CERT. 2023. Cybersecurity and Infrastructure Security Agency. [Online] Available at: https://www.cisa.gov/ [Date of access: 2023].
ICS-CERT. 2016. ICS-CERT Annual Assessment Report FY 2016. US Department of Homeland Security, National Cybersecurity and Integration Center (NCCIC).
IEC-62443-4-1. 2018. EN IEC 62443-4-1:2018 – Security for industrial automation and control systems, Part 4-1: Secure product development lifecycle requirements, Brussels. CENELEC.
IEC-62443-4-2. 2019. EN IEC 62443-4-2:2019 – Security For Industrial Automation And Control Systems, Part 4-2: Technical Security Requirements For IACS Components, Brussels. CENELEC.
IEEE-1686. 2023. IEEE 1686, IEEE Standard for Intelligent Electronic Devices (IED) Cyber Security Capabilities, New York. IEEE.
ISA, 2024. ISA/IEC 62443 Series of Standards. [Online] Available at: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards [Date of access: 2024].
ISO_15408. 2022. ISO/IEC 15408:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security; Parts 1 – 5; Fourth edition 2022-08. ISO/IEC.
ISO_15446. 2009. ISO/IEC TR 15446 Information technology — Security techniques — Guide for the production of Protection Profiles and Security Targets, Geneva. ISO/IEC.
ISO_18045. 2022. ISO/IEC 18045:2022 – Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Methodology for IT security evaluation; Third edition 2022-08. ISO/IEC.
ITSEF-EMAG, 2024. Laboratorium ITSEF. [Online] Available at: https://emag.lukasiewicz.gov.pl/laboratorium-itsef-it-security-evaluation-facility-2/#LaboratoriumITSEF [Date of access: 2024].
KSO3C. 2022. Projekt KSO3C. [Online] Available at: https://www.kso3c.pl/ [Date of access: 2022].
Leszczyna, R. 2018. Cybersecurity and privacy in standards for smart grids – A comprehensive survey. Computer Standards & Interfaces, vol. 56, pp. 62-73.
PCA. 2024. Akredytowane podmioty, laboratoria badawcze. [Online] Available at: https://www.pca.gov.pl/akredytowane-podmioty/akredytacje-aktywne/laboratoria-badawcze/AB%201781,podmiot.html [Date of access: 2024].
Piggin, R. 2013. Development of industrial cyber security standards: IEC 62443 for SCADA and Industrial Control System security. Birmingham.
Rogowski, D. 2013. Software Implementation of Common Criteria Related Design Patterns, Kraków. IEEE, pp. 1147-1152.
Rogowski, D. 2014. Software support for Common Criteria security development process on the example of a data diode. Brunów, Springer International Publishing Switzerland , pp. 363-372.
Rogowski, D. 2018. Identification of Information Technology Security Issues Specific to Industrial Control Systems. Brunów, Springer, Cham: Springer International Publishing, pp. 400-408.
Rogowski, D. 2023. Metoda oceny zabezpieczeń komponentów sieci przemysłowej na przykładzie sterowników przemysłowych. Rozprawa doktorska napisana pod kierunkiem dra hab. inż. Andrzeja Białasa oraz dra inż. Artura Kozłowskiego. Gliwice. Politechnika Śląska.
SOG-IS_Portal. 2024. SOG-IS Senior Officials Group - Information Systems Security. [Online] Available at: https://www.sogis.eu/index_en.html [Date of access: 2024].
SOG-IS. 2010. Mutual Recognition Agreement of nformation Technology Security Evaluation Certificates, Version 3.0, Management Committee, SOG-IS.
Stouffer, K. et all. 2015. NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security Revision 2, Gaithersburg. NIST.
Theron, P., Bologna, S. 2014. Proposals from the ERNCIP Thematic Group, Case studies for the cyber-security of Industrial Automation & Control Systems, for a European IACS Components Cyber-security Compliance & Certification scheme, European Commission, EUR 27098 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen.
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.
Theron, P. et all. 2020. Recommendations for the Implementation of the Industrial Automation & Control Systems Components Cybersecurity Certification Scheme (ICCS), Ispra. European Commission, JRC121520.
Xie, F., Peng, Y., Zhao, W. 2014. Evaluating Industrial Control Devices Security: Standards, Technologies and Challenges. Ho Chi Minh.
Zhou, X., Xu, Z., Wang, L., Chen, K. 2017. What should we do? A structured review of SCADA system cyber security standards. DOI: 10.1109/CoDIT.2017.8102661. Barcelona, pp. 0605-0614.