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

IT/OT Cybersecurity Evaluation – State Of Art

Andrzej Białas

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

Abstract

The Industry 4.0 idea inspires the development of different specialized IT components used to build automation and control systems, like PLD (Programmable Logic Device), SCADA (Supervisory Control and Data Acquisition), HMI (Human Machine Interface), RTU (Remote terminal unit), 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). Such components require security assurance so that they should not be the weakest links of complex industry systems. One of the ways to obtain security assurance is the third party security evaluation and certification. Existing security evaluation schemes and their methodologies are not ready to evaluate numerous components emerging in this domain. For several years new approaches to solve this problem have been developed. Some of them already work, while the most comprehensive ones are under development. The paper includes a review of the main directions of these works. It presents the significance of the EU Cybersecurity Act (CSA) and the initiatives it implied. Existing standards are very important, especially Common Criteria and IEC 62443. They are adapted to new challenges. Equally important are works focused on the preparation of international lightweight certification schemes allowing to get a security certificate in a restricted time horizon.

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

1. Introduction

Today's societies and economies are based on Information Technologies (IT). The IT applications are still growing, implicate new challenges like security, and penetrate into new areas, e.g. automation systems, ambient intelligence, etc.

The Industry 4.0 development rises demand for new components, including cyber-physical ones to build a new generation of systems. Industrial Automatic and Control Systems (IACS) are integrated with company management systems. This way IACS are also connected to the Internet which raises the risk of cyber-attacks on industrial control devices. The integrators and users of automation systems expect that the systems producers will implement reliable mechanisms that would protect OT (Operational Technology) products against cyber-attacks.

Cyber attacks affect also the equipment categorized as the Internet of Things (IoT), embracing the collective networks of connected devices with sensors and processing ability usually connected to the cloud, Internet and application systems. They may be implemented in different environments, like medical and healthcare systems, smart homes, transportation or consumer applications. A specific kind of IoT is distinguished, i.e. IIoT (Industrial Internet of Things), embracing manufacturing, agriculture, military applications, etc.

Digitalization increases cyber security risk across many sectors. There is a need to minimize the risk inherent to the use of IT in the society and economy. One of the ways to do it is IT product security evaluation and certification. The certification obligations are implied by the market needs, the industry, IT owners' risk expectations and by existing EU legislations.

Common Criteria (ISO/IEC 15408, ISO/IEC 18045) is a mature, well established security assurance methodology used for over 20 years in the security evaluation and certification of IT products. Security assurance is related to:

- the rigorous, in terms of security, development, documentation, vulnerability analysis, and testing;

- the independent and thorough evaluation carried out in specialized and accredited laboratories, confirmed by a supervising institution.

Common Criteria is precise, but quite expensive to use and time-consuming for a huge number of IT products emerging on the market each year. These emerging, varied, more or less critical products need security assurance to be used as system components. The existing Common Criteria certification schemes integrating testing (evaluation) labs and certification bodies are not able to perform such certification tasks.

For this reason different bodies: Common Criteria experts, standard organizations, science, industry and consumers try to find new solutions for mass products, which should be evaluated with respect to their security properties and behaviors, because of their criticality. These works are focused on the Common Criteria adaptation, using new industrial standards both de facto and de jure, development of the lightweight certification schemes, etc.

Very important is the activity of the following: 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.

The objective of the paper is to present the main initiatives leading to establishing a unified certification scheme for different IT products, including IACS and IIoT of different security needs.

The aim of the paper is to provide concise information about the current activities focused on the security evaluation and certification of IT and OT components, especially Industrial Automation Control System (IACS) components. Some information is provided for the Internet (Industrial) of Things (IoT/IIoT) components. The review embraces only the key legal acts, standards, papers and reports.

Section 2 concerns the EU Cybersecurity Act and works based on the Common Criteria and IEC 62443 standards, mainly focused on IACS and on works related to the simplified (lightweight) evaluation schemes. Section 3 is focused on IoT and IIoT security evaluation. Section 4 includes conclusions.

2. Towards IACS security evaluation and certification

2.1. Role of the Cybersecurity Act

The Regulation (EU) No 2019/881 called the Cybersecurity Act (CSA) (EU, 2019) concerns two issues:

- it refines the legal authorization of ENISA, defining: objectives, tasks and organisational matters (chapter III); generally the role of ENISA is to establish different European cybersecurity certification schemes focused on ICT products, ICT services and ICT processes;
- it presents a framework for the establishment of these European cybersecurity certification schemes.

Articles 46 through 65 concern the certification framework. Article 51 presents 10 security objectives of European cybersecurity certification schemes cited here directly:

(a) to protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process;
(b) to protect stored, transmitted or otherwise processed data against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process;
(c) that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;
(d) to identify and document known dependencies and vulnerabilities;
(e) to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;
(f) to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;
(g) to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities;
(h) to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident;
(i) that ICT products, ICT services and ICT processes are secure by default and by design;

(j) that ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates."

Article 52 concerns assurance levels used by European cybersecurity certification schemes commensurate with the level of risk existing in the product operational environment, related to the security requirements and functionalities.

Figure 1 presents security levels "BASIC", "SUBSTANTIAL" and "HIGH" defined in the CSA, related to minimized risk and the range of evaluation activities for each of them.

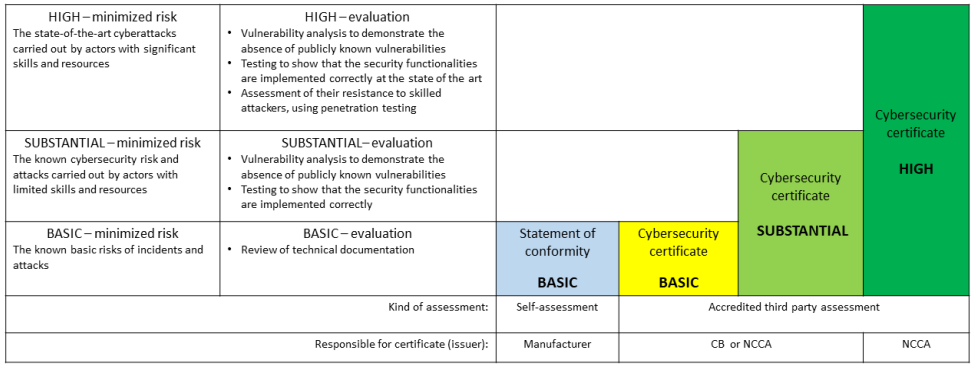

Fig. 1. Security levels implied by the Cybersecurity Act (EU, 2019), (Theron et al., 2020).

Please note that for the BASIC level the manufacturer can issue the statement of conformity after self-assessment or send the product to an independent testing lab for assessment. In the second case the certificate can be issued by a CB (Certification Body) or NCCA (National Cybersecurity Certification Authority).

Article 54 defines elements which ought to be included in the European cybersecurity certification schemes, like: subject matter and scope, purpose, evaluation methods, references to European or national standards, and many other issues. The CSA also presents the rules for:

- Supplementary cybersecurity information for certified ICT products, ICT services and ICT processes (article 55);
- Cybersecurity certification process (article 56);
- National cybersecurity certification schemes and certificates (article 57);
- National cybersecurity certification authorities (article 58);
- Peer review (article 59);
- Conformity assessment bodies (article 60), and many other issues.

The Cybersecurity Act, having a superior nature, creates foundations for different certification schemes. Currently it is focused on ICT products, ICT services and ICT processes. Particular schemes should be defined in details for selected types of ICT products, like IACS or IoT certification.

2.2. Significance of the ERNCIP Report

The ERNCIP Report (Theron et al., 2020), implied by the CSA, includes more technical details and requirements for the ICCS (IACS Components Cybersecurity Certification Scheme).

Section 1 presents acronyms and definitions used in this domain. Section 2 defines the scope of the ICCS, which embraces the following IACS components:

- Automation devices affecting industrial processes;
- PLC (Programmable Logic Controllers) and RTU (Remote Terminal Units);
- Distributed servers affecting PLCs;
- Engineering Workstations to configure RTUs and PLCs;
- Industrial networks that connect the components of a system;
- The Supervisory Control And Data Acquisition system (SCADA);
- The records of the SCADA including the flow of commands and events of an IACS.

The ICCS uses the BASIC, SUBSTANTIAL and HIGH levels. Certification concerns the components, not the IACS systems or their parts. Different approaches can be used in the cybersecurity certification of the IACS components:

- the IEC 62443 based (EC IEC, 2018), (EC IEC, 2019);
- the Common Criteria based (CCRA 2023), (ISO/IEC, 2022a), (ISO/IEC, 2022b);
- lightweight scheme based, like: CSPN (by the French ANSSI) (ANNSI, 2023), BSZ (by the German BSI) (BSI, 2023), BSPA (by Dutch NLNCSA) (NLNCSA, 2023), LINCE (by the Spanish CCN) (CCN, 2020), other under development.

ENISA contributes to the establishment and maintenance of European Cybersecurity Certification Schemes according to the CSA. The Applicants (for certification services) are understood as the entities of various type and scope, e.g. manufacturer, sponsor, developer, producer or supplier of an IACS component, who need certificates for their IT products.

The ERNCIP assumes that the compliance assessment (incl. tests, analyses, reviews) of a designated IACS component with the cybersecurity requirements included in its Component Cybersecurity Profile (CCP) is performed in Certification Bodies (CB) meeting ISO/IEC 17065 and Test labs meeting ISO/IEC 17025, both accredited by a National Accreditation Body.

Section 3 includes an overview of IACS Certification Scheme requirements. The requirements are well structured, numbered and each of them precisely defined. They concern:

- assessment types (more details provided in Figure 1) – self assessment to get the EU statement of conformity or third-party assessment to get the EU Cybersecurity Certificate;
- evaluation activity for each assurance level:
    - for BASIC level:
        - Component Cybersecurity Profile Evaluation;
        - Documentation Review (Basic);
        - Installation;
        - Configuration and Decommissioning Procedures Review;
    - additional for SUBSTANTIAL level:
        - Documentation Review (Substantial);
        - Security Functions Testing;
        - Vulnerability Analysis (Substantial);
    - additional for HIGH level:
        - Documentation Review (High);
        - Development Process Audit;
        - Vulnerability Analysis (High);
        - Penetration Testing;
        - Cryptographic Assessment,
- certificates, statements of conformity – validity, contents.

Section 4 concerns information and artefacts that ought to be delivered by applicants for the assessment/certification process. They are called ENA (Elements Necessary for Assessment) and depend on the claimed assurance level:

- for BASIC level:
    - Component under Assessment (CuA);
    - Component Cybersecurity Profile (CCP);
    - End-user guidance and recommendations;
    - Development process documentation including:
        - Vulnerability management procedure;
        - Patch and obsolescence management procedure;
        - Internal cybersecurity knowledge management procedure;
        - Secure by default and by design strategy;
- additional ENA for SUBSTANTIAL level:
    - Development process documentation including:
        - Configuration management;
        - Life-cycle definition;
        - Incident handlings plan;
    - Robustness testing documentation;
    - Design documentation:
        - Interfaces description;
        - List of parts of the Component under Assessment (CuA);
- additional ENA for HIGH level:
    - Internal Design documentation;
    - Cryptography Information.
    - Access to the development team, the development site and the manufacturing sites shall be provided.

Section 4 also specifies exactly the contents of the Component Cybersecurity Profile (CCP) and other documentation required for each assurance level.

Section 5 is devoted to the evaluation of activities for assessment teams. Please note that currently "there is no single standard that adequately covers the whole set of the evaluation activities defined by the ICCS as necessary to evaluate IACS Components. Therefore, references to applicable standards have been included". The mentioned references concerns the following paths:

- IEC 62443-4-2 (EC IEC, 2019); no official, standardized evaluation methodology exist; the IT Security Association Germany (TeleTrusT) (Fritsch et al., 2019) elaborate own evaluation methodology and makes it publicly available; such works are also performed by the Łukasiewicz-EMAG research team within CyberBEAM project;
- Common Criteria (ISO/IEC 15408 (ISO/IEC, 2022a), ISO/IEC 18045 (ISO/IEC, 2022b)); this methodology should be modified to embraces IACS components;
- Lightweight schemes, like the CSPN, BSPA, BSZ and LINCE.

The ICCS specifies different evaluation activities and related work units concerning:

- Component Cybersecurity Profile Evaluation;
- Documentation Review;
- Installation, Configuration and Decommissioning Procedures Review;
- Security Functions Testing;
- Vulnerability Analysis;
- Development Process Audit;
- Penetration Testing;
- Cryptographic Assessment.

Section 6 includes the specification of the Evaluation and Certification Processes, presenting different flow diagrams describing activities and artefacts during evaluation and roles and relationships between its key actors: Applicant, Test Lab, CB, NCCA, NAB, (National Accreditation Body), and ENISA.

Section 7 includes supporting documents, such as:

- IACS Components Cybersecurity Requirements (ICR) Catalogue;
- IACS Components Cybersecurity Evaluation Report Table of Contents (ICERT);
- IACS Component Cybersecurity Certificates Contents (IC3);
- IACS Component Statement of Conformity Contents.

Annex A shows how relevant are CSA articles implemented in the ICCS and the mapping between the CSA Article 51 and Existing Evaluation Approaches (62443-4-1, 62443-4-2, Common Criteria).

Annex B presents relevant standards: general, e.g. ISO/IEC 17025, risk and management systems evaluation standards, e.g. ISO/IEC 27001, security evaluation standards, like: ISO/IEC 15408, and other relevant ones.

Annex C maps standards to evaluation activities. Annex D concerns the Correspondence of the Agnostic Terminology with IEC 62443 4-2, Lightweight and Common Criteria Certification Paths. Annex E gives some examples of CCP.

The ERNCIP Report is the CSA refinement focused on the evaluation and certification of the IACS components. Different certification schemes can be established on this basis.

2.3. IEC 62443 standard

The IEC 62443 Security for industrial automation and control systems standard includes 13 parts, devoted to general issues, policies and procedures, systems and components, of which two of them are most important for the IACS components development, assessment and certification. They are addressed mainly to developers, consumers, integrators and evaluators.

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.

The Component Requirements (CRs) are derived from the System Requirements (SRs) discussed in IEC 62443-3-3, and SRs are implied by the Foundational Requirements (FRs) defined in part 1 of the standard:

- FR1 Identification and authentication control (IAC);
- FR2 Use control (UC);
- FR3 System integrity (SI);
- FR4 Data confidentiality (DC);
- FR5 Restricted data flow (RDF);
- FR6 Timely response to events (TRE);
- FR7 Resource availability (RA).

The given FR may have several SRs, and SRs are related to CRs.

Generic requirements are numerous, they concern any kind of component and are represented by CR. There are some requirements which are relevant to specific component types only, e.g. software applications type components. Generally, the following types of requirements are distinguished:

- CR Component Requirement (generic);
- SAR Software Application Requirements (specific);
- EDR Embedded Device Requirements (specific);
- HDR Host Device Requirements (specific);
- NDR Network Device Requirements (specific).

The requirements may be enhanced. They are marked as -RE(1), -RE(2), -RE(3). They are added to higher security levels.

Example 2.1: Component requirements for FR1.

FR1 Identification and authentication control has 14 CRs:

- CR 1.1 – Human user identification and authentication;
- CR 1.2 – Software process and device identification and authentication;
- CR 1.3 – Account management;
- CR 1.4 – Identifier management;
- CR 1.5 – Authenticator management;
- CR 1.6 → NDR 1.6 – Wireless access management;
- CR 1.7 – Strength of password-based authentication;
- CR 1.8 – Public key infrastructure certificates;
- CR 1.9 – Strength of public key-based authentication;
- CR 1.10 – Authenticator feedback;
- CR 1.11 – Unsuccessful login attempts;
- CR 1.12 – System use notification;
- CR 1.13 → NDR 1.13 – Access via untrusted networks;
- CR 1.14 – Strength of symmetric key-based authentication.

The wireless access management requirement (CR 1.6) is network-component-specific, similarly to the access via untrusted networks requirement (CR 1.13). For this reason they are replaced by NDR 1.6 and NDR 1.13 respectively.

A security level is defined as a level corresponding to the required set of countermeasures and inherent security properties of devices and systems for a zone or conduit based on assessment of risk. Four Security Levels are distinguished, related to the component capability and embracing 3 security attributes: integrity (I), availability (A) and confidentiality (C): SL 1, SL 2, SL 3, SL 4. They are defined in the context of a given FR.

Example 2.2: FR1, dealing with identification and authentication control, has the following definitions of levels.

- SL1 – Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against casual or coincidental access by unauthenticated entities.
- SL2 – Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against intentional unauthenticated access by entities using simple means with low resources, generic skills and low motivation.
- SL3 – Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against intentional unauthenticated access by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL4 – Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against intentional unauthenticated access by entities using sophisticated means with extended resources, IACS specific skills and high motivation.

Please note that the underlined text is related to the attack potential of intruders considered for a given SL, while the plain text refers to the FR1 context.

Please note that for the given IACS component and the security level, the list of requirements is implied, which can be subject of evaluation, but no standardized evaluation method exists for them currently. IEC 62443-4-2 includes requirements which can be evaluated, in other words, the standard is a source for requirements for IACS.

IEC 62443-4-1 (EC IEC, 2018) concerning security requirements for the IACS component life cycle can also be used. It is based on eight practices:

- Practice 1 – Security management;
- Practice 2 – Specification of security requirements;

- Practice 3 – Secure by design;
- Practice 4 – Secure implementation;
- Practice 5 – Security verification and validation testing;
- Practice 6 – Management of security-related issues;
- Practice 7 – Security update management;
- Practice 8 – Security guidelines.

Each of them has several requirements related to the IACS component for its life cycle phases, e.g.: development, production, delivery, use, decommissioning.

Example 2.3: Requirements related to Practice 2 – Specification of security requirements.

- SR-1: Product security context;
- SR-2: Threat model;
- SR-3: Product security requirements;
- SR-4: Product security requirements content;
- SR-5: Security requirements review.

The requirements included in IEC62443-4-1 can be used to assess how the component was developed, verified, documented, tested, what its properties are, how it can be maintained and used, what design principles were applied, etc. IEC 62443 considers four maturity levels for processes: Initial, Managed, Defined, Improving. The IEC 62443 standard can be applied to both IACS and IIoT components (Leander et al., 2019).

2.4. Common Criteria standard

The basic security assurance methodology is specified in Common Criteria for Information Technology Security Evaluation (CCRA 2023), published also as the family of standards ISO/IEC 15408-x Information technology – Security techniques – Evaluation criteria for IT security (ISO/IEC, 2022a), (ISO/IEC, 2022b).

Common Criteria includes currently 5 parts:

- Part 1: Introduction and general model;
- Part 2: Security functional requirements;
- Part 3: Security assurance requirements;
- Part 4: Framework for the specification of evaluation methods and activities;
- Part 5: Pre-defined packages of security requirements,

and the Common Criteria evaluation methodology (CEM) – ISO/IEC 18045 (ISO/IEC, 2022b).

Part 2 of the CC standard includes CC components, which express elementary security functional requirements (SFRs) used to specify the IT product security behavior. Part 3 of the CC standard includes CC-components, which express elementary security assurance requirements (SARs) claimed for this product. The components described in both parts are grouped by families, which, in turn, are grouped by classes, e.g.:

- the "FDP" functional class concerns the user data protection, its family "FDP_ACC" concerns the access control policy, and the family component "FDP_ACC.2" expresses the issue of "Complete access control";
- the assurance class "ATE" concerns tests, its family "ATE_COV" (coverage of the implemented security functions by tests) deals with the level of details to which the security functions are tested by the developer; this family has three CC components with rising and cumulating rigour: "ATE_COV.1 Evidence of coverage", "ATE_COV.2 Analysis of coverage", "ATE_COV.3 Rigorous analysis of coverage"; the assurance class ALC Life-cycle support includes many similar requirements to IEC 62443-4-1.

An IT product or its part being the subject of evaluation is called the Target of Evaluation (TOE). There is evaluation evidence assigned to each SAR component. It is submitted by the developer and assessed according to CEM. The degree of effort dedicated to the TOE development depends on its scope (less or more of the IT product is evaluated), depth (fewer or more design and implementation details are considered), and rigor (a more or less structured and formal approach is applied).

Security assurance is measurable using EALs (evaluation assurance levels) in the range from EAL1 to EAL7. The TOE security functionality is specified with the use of SFRs, and is implemented and evaluated according to the claimed EAL expressed by the set of SARs. The CC "SAR components" are related to the CEM "subactivities". The latter are divided into evaluation actions refined by work units. The role of the evaluator is to examine the evidence and/or the product behavior and to assign verdicts (pass/fail/inconclusive) to the evaluation actions.

The CC methodology is devoted to IT products, though it may be not enough to consider certain issues related to specific products, including IACS or IIoT components. The CC methodology has open character – the missed

SFRs or SARs can be defined and added as the extended components. For such products a specific evaluation method can be defined according to Part 4 of the standard. Apart from these mechanisms, the specific security profiles can be defined.

2.5. Lightweight schemes

Please note that the Common Criteria methodology is not explicitly designed to be used in a fixed time. The Common Criteria methodology is detailed, but not effective for certain cases, e.g. when the certification time and costs should be predictable and low. It is especially important for emerging products, which should be quickly launched on the market. Lightweight schemes concerns low or medium security levels.

In response to these needs, several national, lightweight evaluation schemes are elaborated: CSPN (ANNSI, 2023), BSZ (BSI, 2023), BSPA (NLNCSA, 2023), LINCE (CCN, 2002).

Lightweight schemes assume 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. The comparison of these lightweight schemes is placed in the (Ruiz, 2023). The author considers workloads, duration, reports, lab accreditation, required evidences, and evaluation activities.

The FITCEM (EN 17640) methodology (CEN/CENELEC, 2022) is claimed as the first cybersecurity methodology created to meet the European Cybersecurity Act (CSA) (JTSEC, 2023). It was developed by the CEN/CENELEC JTC13 WG3 (CEN/CENELEC, 2023) which is working on the evaluation methodology on the EU level. FITCEM is flexible and for this reason it can be customized to meet the needs of the different schemes and self-evaluation. The following evaluation tasks are defined,

- Completeness check;
- FIT Protection Profile Evaluation;
- Review of security functionalities;
- FIT Security Target Evaluation;
- Development documentation;
- Evaluation of TOE Installation;
- Conformance testing;
- Vulnerability review;
- Vulnerability testing;
- Penetration testing;
- Basic crypto analysis;
- Extended crypto analysis.

The task details depend on the claimed CSA security level. Some activities are optional. The developer should provide a FIT Security Target and a Secure User Guide. The structures of the FIT Security Target and the FIT Protection Profile are placed in annexes A and B. Annex C specifies acceptance criteria with respect to: Identification, Authentication Control, and Access Control, Secure Boot, Cryptography, Secure State After Failure, Least Functionality, and Update Mechanism. The FITCEM methodology and its particular tasks have some parameters, which should be configured, e.g.: number of samples, availability of open samples, source code, tasks workload, tasks duration, etc. (Annex E). Annex F describes the method of attack potential calculation similar to the method used in CC. Annex G concerns reporting.

3. Towards IoT/IIoT security evaluation and certification

Currently several schemes based on the comprehensive IoT testing against potential attacks and vulnerabilities are elaborated by companies or organizations.

The CTIA company established a cybersecurity certification program for IoT devices (CTIA, 2021). It can be considered an industry baseline for device security on wireless networks. CTIA cooperates with several Authorized IoT Cybersecurity Test Labs. The CTIA program is based mostly on the security NIST, RFC standards.

The CTIA Cybersecurity Certification Program is organized in basic three levels. The first level identifies core IoT device security features, the second and third supplement it by more sophisticated elements:

- Level 1 IoT Cybersecurity Tests – Terms of Service and Privacy Policies, Password Management, Authentication, Access Controls, Patch Management, Software Upgrades;
- Level 2 IoT Cybersecurity Tests (added to Level 1) – Audit Log, Encryption of Data in Transit, Multi-Factor Authentication, Remote Deactivation, Secure Boot, Threat Monitoring, IoT Device Identity;

- Level 3 IoT Cybersecurity Tests (added to Level 2) – Encryption of Data at Rest (data stored on the device), Digital Signature Generation and Validation, Tamper Evidence, Design-In Features.

The ioXt Alliance (ioXt Alliance, 2024) is focused on building confidence in the Internet of Things products. It integrates different stakeholders across the world. IoT product manufacturers and developers can gain formal certification based on the established ioXt Certification Program and the net of authorized test labs. The ioXt self-certification is also possible. The method is based on several profiles, e.g.: Base profile, Android profile, Residential camera profile, Smart speaker profile, Mobile application profile. The given profile defines the devices which may be certified using the profile, a threat model, and a test plan. The base profile covers all devices which are not covered by another profile.

The Global Platform develops the Security Evaluation Standard for IoT Platforms – SESIP (GPT, 2021). The standard concerns combination of hardware and software that provide a runtime environment for a connected application, understood as software developed by an IoT vendor, implementing an IoT end-user use case based on the platform. SESIP is based on the Common Criteria approach. The SFRs from Part 2 were replaced by requirements relevant to the IoT environment. The SARs from Part 3 were refined and some specific SARs were added. The EALs were replaced by the scale: SESIP1 to SESIP5 levels. Global Platform provides certification services based on its own standard.

The paper (Baldini et al., 2016) proposes the certification process of IoT based on comprehensive testing, related to the Horizon 2020 ARMOUR project, embracing:

- risk analysis in the environment, where IoT will operate at a required assurance level (analogy to Common Criteria EAL);
- analyzing knowledge related to potential threats and vulnerabilities in this environment;
- test suites generation using the TTCN-3 (Testing and Test Control Notation v. 3) notation;
- testing based on the MBT (Model-based testing) concept, the use of test adaptors (wrappers) and testbeds.

The updated, more formalized and related to the existing standards version of this framework was presented in the paper (Matheu et al., 2019). It is based on the ETSI security assessment and testing methodologies.

The next two approaches based on IEC 62443 are under development.

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). The authors determine the applicability of the IEC 62443 standards and certifications to IIoT components and systems by the examination of the IEC 62443 requirements and methods used to validate these requirements during certification of IIoT components.

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). No official reports have been published so far.

4. Conclusions

The IT products requiring security certification, like IACS, IIoT/IoT are varied, still evolving and working in different operational environments (Boyes et al., 2018). The evolution is observed from hardware-based models to data-service-based models. Also the threats characters are changing. The number of all possible attack points or attack vectors is rising too. These issues ought to be considered in the development of certification methods and schemes for these products.

The certification methods and schemes are currently developed under auspices of different world players – organizations representing industry, standard authorities, security authorities, governments and EU. Due to their fragmentation, the existing evaluation methods and schemes should be ordered and unified to extend their compatibility and range. The review identifies a broad range of methods: detailed and complex or lightweight, based on international standard or owned by companies, matured or emerging.

The European CSA is a leading initiative. It defines the general framework in which the certification schemes for different kinds of ICT products, ICT services and ICT processes can be designed and established. This approach allows to order and unify certification issues across Europe and decrease the fragmentation of efforts in this domain. A very important role in this task is played by IEC, CEN/CENELEC JTC13 WG3 and ENISA.

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

ANSSI. 2023. Certification Sécurité de Premier Niveau (CSPN). https://www.ssi.gouv.fr/administration/produits-certifies/cspn/ (accessed on 22 December 2023).

Baldini, G., Skarmeta, A., Fourneret, E., Neisse, R., Legeard, B., Le Gal,l F. 2016. Security certification and labelling in Internet of Things. 2016. IEEE 3rd World Forum on Internet of Things (WF-IoT 2016), Reston, Virginia. USA. Institute of Electrical and Electronics Engineers (IEEE), 627 – 632.

Boyes, H., Hallaq, B., Cunningham, J., Watson, T. 2018. The industrial internet of things (IIoT): An analysis framework. Computers in Industry 101, 1–12.

BSI. 2023. Accelerated Security Certification (BSZ). https://www.tuvit.de/en/services/cyber-security/bsz/ (accessed on 18 December 2023).

CCN – Centro Criptológico Nacional. 2002. Guía de Seguridad de las TIC CCN-STIC 2002 Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE). https://www.jtsec.es/files/CCN-STIC-2001_0.1.pdf (accessed on 18 December 2023).

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.

CEN/CENELEC. 2023. Digital Society. https://www.cencenelec.eu/areas-of-work/cenelec-sectors/digital-society-cenelec/cybersecurity-and-data-protection/ (accessed on 9 January 2024).

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-sBhAoEiwArqlGPowCJmz2d5wiqDFC7QD8ER5x14g84SHIko2xh-nXbt5wuzYnYm OIZhoC-xUQAvD_BwE (accessed on 8 January 2024).

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

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

ISO/IEC. 2022. 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).

Leander, B., Causevic, A., Hanson, H. 2019. Applicability of the IEC 62443 standard in Industry 4.0 / IIoT. ARES '19: Proceedings of the 14th International Conference on Availability, Reliability and Security, Pages 1–8.

Matheu, S.N., Hernandez-Ramos, J.L., Skarmeta, A.F. 2019. Toward a Cybersecurity Certification .Framework for the Internet of Things IEEE Security & Privacy, May/June 2019, pp. 66-76.

NLNCSA. 2023. BSPA – The Dutch Baseline Security Product Assessment. https://www.riscure.com/service/baseline-security-product-assessment/ (accessed on 18 December 2023).

Ruiz, J. 2023. Analysis and comparison of lightweight evaluation methodologies. https://www.jtsec.es/papers/Others/analysis-comparison-of-lightweight-evaluation-methodologies.pdf (accessed on 18 December 2023).

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.