Security certification experience for industrial cyberphysical systems using Common Criteria and IEC 62443 certifications in certMILS

Andreas Hohenegger, Gerald Krummeck, atsec information security GmbH, Janie Baños, Alvaro Ortega, DEKRA, Michal Hager, Jiri Sterba, Elektrotechnický zkušební ústav s.p. (EZU), Tomas Kertis, Petr Novobilsky, Jan Prochazka, Q-Media s.r.o., Benito Caracuel, Ana Lourdes Sanz, Francisco Ramos, Schneider Electric, Holger Blasum, Mario Brotz, Caspar Gries, Torsten Vögler, SYSGO GmbH, Jan Neškudla, Jan Rollo, SYSGO s.r.o., Lisa Burgstaller, Martina Truskaller, Klaus-Michael Koch, Technikon, Reinhard Hametner, Sandro Rauscher, Peter Tummeltshammer, Thales Austria, Frank Golatowski, Thorsten Schulz, Universität Rostock

Abstract— **Security concerns become increasingly important in safety-critical industrial cyberphysical systems. Different options for security certification exist. We describe a Common Criteria certification for a MILS separation kernel, and IEC 62443 analysis and certifications for the smart grid, railway and subway pilots using the MILS approach in the research project certMILS.**

I. Introduction

Previously isolated cyberphysical systems now are connected to the Internet. For instance, for user/passenger comfort as well as operational efficiency, many means of transportation (airplanes, trains, cars, ships), energy, and manufacturing are networked.

This gives rise to security concerns in highly critical systems and their infrastructure. Addressing these concerns requires new technical solutions and certifications to assure mitigation of risks. The approach established in the research project certMILS ("Compositional security certification for medium- to high-assurance COTS-based systems in environments with emerging threats") uses a compositional design (MILS, "multiple independent levels of safety / security" [1]) and a compositional security certification to research re-usage of a certified COTS product, the separation kernel.

We evaluate this approach with project partners Q-Media (Cz), Schneider Electric (Es) and Thales Austria (At) acting as system integrators for pilot systems (demonstrators) in the subway, smart grid, and railway domain. In this paper we report on the certification experiences in Common Criteria for the separation kernel and IEC 62443-4-1 / IEC 62443-4-2 according to the IECEE CB scheme for the pilot systems. Research questions comprise: (1) understand via learning-by-doing re-use of existing safety experience and artifacts for security as well as the effort still needed and (2) understand how a separation kernel can be used to ease IEC 62443 certification. Here we deal with (1); question (2) is focus of a planned future publication [2].

The following section describes how we selected the respective standards, followed by the individual descriptions for Common Criteria and IEC 62443. In Section VI we conclude with lessons learnt highlighting the differences in the certification approaches and what it means to target real-world certifications in a research project.

II. Choice of standards

The employed separation kernel was certified to Common Criteria for Information Technology Security Evaluation (CC) [3]: The rigor of the CC suggests to focus on a small system/product or subsystem of a product [4]. The MILS separation kernel is such a product suitable for CC.
In the domain of industrial automation and control systems (IACS), the standard IEC 62443 considers the security of entire plants and takes strongly into account the constant changes that need to made to a plant, by putting great emphasis on the processes during the life cycle of an IACS.

For instance, risk assessment is not just carried out at the beginning, but continuously repeated to achieve improvement. Railways and the track-side networks as distributed systems have a complexity comparable to IACS, and CENELEC's EN 50701 (prTS) [5] is based primarily on the IEC 62443 standard in the field of cyber-security. As the pilots are in the IACS domain (smart grid) and railway domain (railway and subway pilots), we chose IEC 62443-4-1 [6] and IEC 62443-4-2 [7] as certification standard. IEC 62443 has different certification schemes, such as: (1) IECEE Industrial Cyber Security Program [8], (2) ISASecure IEC 62443 Certifications [9], (3) exida IEC 62443 Cyber Security Certification Programs [10].

With one of our consortium members, EZU (Cz), playing a major role in IECEE scheme development, we chose (1). This choice was further supported by specifications of the scheme itself. The IECEE CB scheme for cyber-security based on IEC 62443 standards brings many unique advantages:

- The scheme is operated under IECEE, which is a popular scheme for standardization.
- The applicant can choose requirements that will be in the scope of the assessment.
- The statement is made for the time of the assessment and for a concrete version of the product.

III. Common Criteria for separation kernel

The separation kernel is certified according to CC, demanding us to fulfil different requirements such as describing the security properties via a document called "security target" (ST) and carrying out conforming development, guidance, life-cycle, testing and vulnerability analysis evaluation activities.

The first step is to create an ST for the target of evaluation (TOE) by the developer (SYSGO, project member), which according to the CC includes the following sections:

- Security problem definition, identifying the assets, attackers and the threats.
- Derivation of security objectives that counter the threats.
- Derivation of security functional requirements (SFRs) that formalize the security objectives.
- Rationales showing that the security objectives mitigate all identified threats, validating that all security objectives are covered/fulfilled by the derived SFRs.

In the next step we produced guidance, development and lifecycle artifacts. The certification lab (atsec, project member) demonstrated that they are correct in the course of an evaluation. Similar to the IEC 62243 certifications (see Sections IV and V), we were able to re-use many documents from a previous safety certification, e.g., for functional specification and general design.

Functional specification: The functional specification defines the TOE security functionality interface (TSFI), that is how system functionality is invoked, including what happens when invalid input is given (normal behavior, erroneous behavior). For a general-purpose operating system such functional specification is often provided by user documentation, e.g., in another evaluation for a Linux distribution, evaluators had used "man" (manual) pages [11]. For the separation kernel, we were able to use formal software requirements also used in safety contexts, e.g., in order to demonstrate 100% code coverage (needed in avionics, but not for CC). Using existing safety requirements, for us, meant better reuse of traceability to test cases.

System design: Popular software design approaches use decomposition into components and connectors [12]. The CC follows such approaches by asking to describe how the TOE can be decomposed into subsystems, and what the relations between the subsystems are. In our case, the main subsystems of the separation kernel are the PikeOS Microkernel and the PikeOS System Software (PSSW) [13]. A subsystem interaction consists in that the user-space PSSW requests microkernel functionality via system calls. In the next step, subsystems are broken down into modules and the developer has to describe interactions of modules: for instance, when a task is created dynamically, then some memory manager has to provide memory for data structures managing that task, a stack area, etc. Unlike many safety standards that follow a more homogeneous approach, the CC encourages the developer to mark certain parts as SFR-enforcing, SFR-supporting and SFR-non-interfering, depending on whether the code directly enforces an SFR, supports it, or does not interfere with it.

Security architecture: While safety standards have a general notion of "robustness", the CC require the developer to demonstrate certain specific non-functional security properties [14], in particular domain separation, secure initialization, self-protection and non-bypassability. Domain separation means how the TOE maintains different security domains for users. Self-protection argues that a user cannot successfully attack the TOE itself. Non-bypassability argues that protection mechanisms are complete and secure initialization asks the developer to show how the TOE reaches a secure initial state after power-up. Providing a MILS separation kernel, we have a strong case for separation of security domains, which are mapped to the partitions of the separation kernel. The security architecture maps to the implementation of the separation kernel partitions, how these security domains are consistently created (secure initialization) and maintained (domain separation). This includes how we use the MMU for address space protection, so that an application running in one partition cannot interfere with an application running in another partition. TOE self-protection means demonstrating that applications cannot attack the TOE itself. Non-bypassability arguments look at *all* interfaces accessible in the operational environment, including their detailed mechanisms and parameter, handling and argues that there are no means to circumvent them.

Testing and vulnerability analysis: Verification in CC is performed in three ways:

- Functional testing by the developer,
- independent testing performed by the CC evaluator, and
- penetration testing as part of the vulnerability analysis also performed by the CC evaluator.

For the separation kernel, the TSFIs at the attack surface are the system calls and APIs exposed by the kernel and PSSW system software. Particular emphasis is given to TSFIs that are enforcing and supporting the security functionality enumerated by SFRs in the ST. A test coverage analysis known as ATE_COV shows that TSFIs and SFRs are tested and another analysis known as ATE_DPT proves that the internal interfaces between modules are tested. This may include indirect testing via invocation of external interfaces, and further tracking of control flow across the internal interfaces. In independent testing, the evaluator reproduces a subset of test cases and performs own tests that may be variations thereof. The aim of the vulnerability analysis and pen-testing is to make sure that the separation kernel is free from any known security vulnerabilities. The evaluator uses public databases of known vulnerabilities (e.g. Common Vulnerability Enumeration / CVE) to find any applicable vulnerabilities and perform pen-testing to find out if such vulnerability exists in the separation kernel. In addition, the activity requires flaw hypotheses based on the evaluator's knowledge of TOE internals, gathered in prior evaluation steps, and demonstrates that they cannot be realized with given capabilities of an assumed attacker (white-box pen-testing).

Other: We also have to submit user documentation (guidance) - where it is important that the capabilities and limitations of the product with respect to security functions are properly laid out - and life cycle artifacts (not a focus of this paper).

IV. IEC 62443-4-1

A. Applied process

In the first step of the process, the applicant submits an application to the certification body. The certification body assesses the application for conformance. After business and contractual matters are solved, the applicant receives the Test

Report Form (TRF) and its annex, plus questionnaire. The questionnaire provides the certification body with information necessary for the next step – scoping of submittal. It specifically provides the information of requirements and maturity levels chosen, identification of certification scenarios and specifications of the {product, process, service, solution} that is going to be assessed.

In the next phase, the applicant completes the applicable portions of a TRF and provides evidence in support of the capabilities that are intended to demonstrate compliance to the selected requirements. After that, each selected IEC 62443 security requirement is evaluated against the supporting evidence supplied by the applicant to determine compliance by certification body.

The results of the assessment are gathered in the TRF and its annex. In this form it is also presented to the applicant. The possible result for each requirement is one of the following: pass, fail, N/E (not evaluated).

The certification body issues a certificate for requirements that have been met. Requirements for these certificates are again defined by IECEE – all certification bodies are obliged to follow these instructions. They are defined in IECEE OD-2037 5 (Edition 3.2, 2019-06-05) IECEE Test Certificates.

B. Examples

The products that we certify for security are safety-critical products that have already undergone some safety certification and/or development. Often artifacts developed for safety-critical development can be re-used for IEC 62443-4-1. For instance, certMILS partner Q-Media is using an internal certification framework to cover simultaneously EN 50126, IEC 61375, prTS 50701 and IEC 62443 [15]. A gap analysis between IEC 62443 and IEC 61508 has been done in [16].

For instance, IEC 62243-4-1 SM-1 ("development process") stipulates that "*a general product development/ maintenance/ support process shall be documented and enforces that is consistent and integrated with commonly accepted product development processes that include, but are not limited to: (a) configuration management with change controls and audit logging; (b) product description and requirements definition with requirements traceability; (c) software or hardware design and implementation practices, such as modular design; (d) repeatable testing verification and validation process; (e) review and approval of all development process records; and (f) life-cycle support.*" As shown in Table 1, for this, pilots refer to safety relevant documentation made during safety critical certification, such as offer-creation-process documentation (smart grid), a collection of safety and security architecture documents (railway), and EN 50126 evidence (subway).

Table 1: Example: Evaluation evidence for IEC 62443-4-1 SM-1 "Development process", compliance of the pilots

Smart grid	- The offer creation process documentation includes the requirements, specifications, design, verification and validation of the product, along the different stages for the development. - Coverage analysis that indicates how the requirements of IEC 62443-4-1 SM-1 are met. - Evidence of ancillary certifications that the company did in the past.
Railway	- Verification of the information from the client provided in the columns "Declared Maturity Level", "Conformity Statement", "Applicable Component" and "Conformity Evidence" in the document "iec62443_4_1a_Compliance Checklist_filled_by_Thales.xls" - Analysis of the SM-1 requirement in IEC 62443-4-1 and its justification in this standard - Assessment of the content of the "Conformity Statement" column, in which the client briefly described how he meets the SM-1 requirement. It included the definition and implementation of individual stages of development of the TAS PLF Core SW 2.4.1 component of the TAS Platform system - Verification of the information given in the "Conformity Evidence" column in the provided documents (CMP, FL, SSRS_Sec, VCRM, SSDD, Sec_Arch, IVP, VQP, DOC_Plan, QMP, IVP, PSEMP) These documents are documenting the whole life cycle of the component development - The assessment of compliance with the SM-1 requirement continued with the verification of the compliance of the individual phases of component development with the generally accepted ISO 9001 standard
Subway	- verification of the information provided by the client in the columns "Declared Maturity Level", "Conformity Statement", "Applicable Component" and "Conformity Evidence" in the document "Documentation iec62443_4_1.xlsx", - analysis of the SM-1 requirement in IEC 62443-4-1 and its justification in this standard, - assessment of the content of the "Conformity Statement" column, in which the client briefly described how he meets the SM-1 requirement. It included the definition and implementation of the development life cycle, also respecting EN 50126 components called Subway pilot R01-401, - verification of the information given in the "Conformity Evidence" column in the provided documents (H07 QS10 Product Development, Chapter 7 and Project Management H0002), which are documenting the whole life cycle of the component development, - the assessment of compliance with the SM-1 requirement continued with the verification of compliance of the individual phases of component development with the generally accepted ISO 9001 standard, - Based on the above procedures and information, the requirement of SM-1 "Development process" was assessed as met.

For the railway pilot, penetration testing was carried out by the security evaluator DEKRA and potential vulnerabilities were analyzed by Offensive Security Certified Professional (OSCP) certified personnel. Thales supplied a penetration testing rack equipped with system boards of all necessary processor architectures and specific configurations for the TAS platform. Dedicated DEKRA security experts extensively tested the systems over the course of ten full workdays.

The evaluation was accomplished focusing on two 'groups': **Device** and **Network** evaluation. On the one hand, "Device Evaluation" focuses on the vulnerability analysis carried out over Thales specific device firmware and its services, including potential misconfiguration or sensitive information leaks among others. On the other hand, 'Network Evaluation' focus-

es on the analysis of the information transmitted through the connected network and how it could potentially derive vulnerabilities in terms of confidentiality or integrity weaknesses.
Used tools for both cases of evaluation include various publicly available scanners and frameworks specifically used for offensive security testing such as:

- Kali Linux OS: a Debian Linux based distribution combining (nearly) all necessary tools needed for extensive penetration tests, data forensics and ethical hacking.
- Nmap: a free and open source utility for network service discovery, enumeration and security auditing.
- Metasploit and its built-in exploit-database: a complete penetration testing, information gathering (such as used configuration) and backdoor testing framework using highly configurable public domain exploits and payloads for every architecture and major operating systems.
- THC-Hydra: a multi-purpose login cracker for nearly all widely-used network protocols.
- Snmpwalk, snmp-check: enumeration and security testing of SNMP enabled devices.
- Tcpdump, Wireshark: advanced network protocol analyzers.
- Ike-scan: a command-line tool that uses the IKE (Internet Key Exchange) protocol to discover, fingerprint and test IP-Sec Virtual Private Network servers.
- Lynis: helps with auditing systems running UNIX-alike systems (Linux, macOS, BSD), and providing guidance for system hardening and compliance testing.

All of these tools had been excessively used by the implementer/editor beforehand to find vulnerabilities, configuration errors, or simply conduct exploit-tests even while regression-testing the TAS-Platform.
Regarding pen-testing of the Smart Grid pilot, the evaluation laboratory carried out a set of tests, which checks for potential vulnerabilities in published services such as the SFTP server or the DNP3 protocol. In addition, possible privilege escalations were carried out to prove that there are no ways to attain the most privileged user (root), as well as:

- Several public 'exploits' of kernel and services were tested.
- Hidden services recognition on network ports, as well as services versions.
- Analysis of non-protected sensible information.
- Analysis of potential manipulated binary configuration files.
- Privilege escalation: Exploitation of root running services, exploitation of SUID executables, exploitation of 'cron' service jobs, traversal directories pivoting.

V. IEC 62443-4-2

IEC 62443-4-2 [7] consists of functional requirements. Here certMILS pilots chose to cover most of the available functional requirements: The railway pilot has done a IEC 62443-4-2 certification, the subway pilot is heading for a IEC 62443-4-2 certification, and the smart grid pilot did a gap analysis for what is needed for fulfilling IEC 62443-4-2.

A. Applied process

For the smart grid, once evaluators had enough knowledge of remote terminal unit (RTU) devices, the evaluation of the security artifacts stage began. At first instance, both the evaluation laboratory and the manufacturer drew a conclusion about which IEC 62443-4-2 requirements apply to the evaluation stage. After reviewing all the IEC 62443-4-2 requirements, they selected the more appropriate requirements for the Smart Grid pilot. As an example, CR2.4 "Mobile code" was not selected due to the pilot lacking an execution environment to launch such technologies. Similarly. the railway pilot chose "not applicable" for the requirement CR1.6 "Wireless access management" because the TAS-Platform does not support wireless devices at all. It chose "not implemented" for CR3.11 "Physical tamper resistance and detection", because Thales delivers the bare metal hardware device and the complete OS separate from it, with the OS being unconfigured and all storage devices being empty at first. It is the customer's obligation to provide appropriate physical security to their premises and/or devices after configuring and deploying the OS on the hardware.

B. Examples

As shown in Table 2, for testing a functional requirement, typically, appropriate tests are formulated and their results are recorded. EZU applied their ICT Testing Infrastructure for Auditors for both the railway and the subway pilots.

Table 2: IEC 62443-4-2 CR-1.1 "Human user identification and authentication", an example of evaluation of requirement not involving the separation kernel: compliance of the pilots

Smart grid	The manufacturer sent the RTU equipment to DEKRA lab for performing the testing/pentesting. User manuals are also provided for the evaluators gain experience in the use of the RTU. The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures. In order to evaluate such requirement on the Smart Grid pilot, the evaluator has identified all interfaces on the RTU device which provide functional manageability. The evaluator identified SSH/SFTP interface, a web-application interface, and a console interface (through a serial port). The evaluation laboratory requested a list of all pre-defined users and roles to the manufacturer device. Such list contains a set of users which are associated with a set of roles. Each role has pre-defined permissions to carry out specific tasks. The provided default users for the RTU are the following: Viewer, Operator, Engineer, Installer, SecurityAdmin, SecAud and RbacMnt. The users are assigned one of the following roles (at least): VIEWER, OPERATOR, ENGINEER, INSTALLER, SECADM, SECAUD and RBACMNT, and each one is assigned privileges such as: CONF_DB, WEBSERVICES, RESET, etc. A role can provide 'read', 'write' and/or 'access' function for each of the privileges. The privileges which have been tested regarding 'human identification and authentication' are the following: - WEBSERVICES, allows access through the web interface, to a user with some of the following roles: 'VIEWER', 'OPERATOR', 'ENGINEER', 'INSTALLER' and 'SECADM'. - SSH, allows access through SSH/SFTP interfaces to

	those users with some of the following roles: 'ENGINEER' and 'INSTALLER'. - OS_SHELL, these privileges are related to the SSH privilege. When a role is assigned OS_SHELL, the user will receive a usual '/bin/sh' terminal through the SSH interface. Such interfaces have been developed by the manufacturer and provide a menu with commands that give information about the RTU. 'OS_SHELL' privilege is assigned to the 'ENGINEER' role. The evaluator has tested two paths: Check that users with appropriate privileges to access through the interfaces are allowed and prove that users without privileges are not allowed.
Railway	The assessment of this requirement has been performed in the following steps: - Verification of the client's indication of interest for assessment in document "62443-4-2_Applicability_filled_by_Thales.xlsx" - Verification of the information provided by the client in the columns "Conformity Statement" and "Conformity Evidence" in the document "iec62443_4_2a-worksheet (TRF) final_filled_by_Thales.xlsx", - Analysis of the CR 1.1 requirement in the IEC 62443-4-2 standard (including a reference to the SR 1.1 requirement in the IEC 62443-3-3 standard, ed. 1.0 2013-08) and their justification in both standards, - Assessment of the content of the "Conformity Statement" column, in which the client briefly described how he meets the CR 1.1 requirement by using the Linux operating system, which includes user access control and authentication functionalities (especially /etc/passwd, /etc/ /group and /etc/shadow), and using the Pluggable Authentication Module (PAM) to implement a security policy - The assessment of compliance with the CR 1.1 requirement continued with the verification of the mentioned functionalities for access control and user authentication in the Ubuntu 18.04 LTS operating system installed in TiICTa (ICT Testing Infrastructure for Auditors) by EZÚ, - Verification of the information given in the column "Conformity Evidence" in the provided document "16_TAS_Platform SecurityHandbook_ed05RL.pdf", chapter 3.5 containing information on the used PAM modules, recommended configuration and documentation.
Subway	The assessment of this requirement has been carried out in the following steps: - verification of the client's indication of interest for assessment in document "62443-4-2 _Applicability_QMA.xlsx", - verification of the information provided by the client in the columns "Conformity Statement" and "Conformity Evidence" in the document "Documentation iec62443_4_2.xlsx", - analysis of the CR 1.1 requirement in the IEC 62443-4-2 standard (including a reference to the SR 1.1 requirement in the IEC 62443-3-3 standard, ed. 1.0 2013-08) and their justification in both standards, - assessment of the content of the "Conformity Statement" column, in which the client briefly described how he meets the CR 1.1 requirement by using standard functionality for assigning users and user rights in Linux, including the use of LDAP (Lightweight Directory Access Protocol) for network system management, - the assessment of compliance with the CR 1.1 requirement continued with the verification of the mentioned functionalities for access control and user authentication in the Ubuntu 18.04 LTS operating system installed in TiICTa by EZÚ, - verification of the information given in the "Conformity Evidence" column related to the initialization of the relevant daemon in the VMIT configuration file in the ElinOS (Linux) operating system documentation.

Moreover, some functional requirements explicitly reused assurance provided by the separation kernel. The functional requirements were mainly in the functional groups for restricted data flow and resource availability [15].

VI. Conclusions and Lessons Learned

A. Overall results

The context of a research project was helpful for the world's first IECEE CB IEC 62443-4-1 certification because it offered resources to follow the IECEE CB standardization process closely and at the same time to find partners to try it out, with part of the risk being mitigated by the research context.

B. Reuse of artifacts from previous safety certifications and coexistence of safety and security certification

Certification is about presenting correctness arguments to an evaluator in an understandable form. There are some commonalities here, and in all cases (CC and pilots) we were able to re-use development and testing artifacts from safety standards such as design and interface documentation. E.g. in the case of the separation kernel, a requirement engineering database was used to record traceability relations over high and low-level requirements to source code and test cases and this could be reused for safety. However, we had to make security-specific additions (e.g., threat modelling, security architectures, penetration testing, specific security test suite for IEC 62443 that is being developed by EZU, specific user guidance for safety). The necessity to think like an attacker puts focus on trust boundaries: for instance, OS system calls consist of kernel space and a user space part, however the user space part cannot be protected from the user and, in comparison to a safety certification, a security certification has to ensure that all security checks are on the kernel space side and not on the user space side. Another instance are completeness concerns, which are less relevant in safety than in security: an attacker will actively try to attack undocumented APIs or invalid parameters, whereas in requirement engineering for safety the focus in on positive functionality, but not on the absence of undocumented side effects. On the other hand, to ensure that safety aspects are formally covered in the security certification context, the railway pilot chose to integrate them as "Common Component Security Constraints" defined as "CCSC 1: Support of essential functions" and "CCSC 2: Compensating countermeasures".

If one does safety and security certification on the same product, then a practical challenge is that different documents may need updates from different sources (e.g., updated safety certification may need to be reviewed in the security certification again).

C. Cross-comparison CC and IEC 62443

We used the CC for evaluation of the separation kernel and IEC 62443 for the evaluation of the pilots. The CC it is split

across national interpretations the IEC 62443 it is split across certification schemes. In IEC 62443, certification bodies can be commercial entities, in CC they are national authorities. Note that in CC, for evaluations that are not targeting high evaluation, certifications by commercial entities are under discussion [17]. In both types of evaluations, the application starts with a generic scoping. E.g., for IEC 62443 with the selection of functional requirements. In CC, the effort for an ST is generally higher because functional requirements have to be adapted for a specific product in the ST. However, by following CC protection profiles (PP), the efforts can be reduced. A certMILS PP draft has been produced within this project [18] [19]. A difference is that in a CC evaluation the vendor must provide a set of documents (ADV, ASE, AGD, ALC) defining the installation steps of the TOE, information about all the interfaces to access to the TOE functionalities, information about all systems and subsystems of the TOE, and so on. However, the IEC 62443 standard does not oblige to the vendor to provide such information, so the evaluators face unknown devices without information about them. As the IEC 62443 allows a wide interpretation of the requirements, DEKRA evaluators realized that the vendor should take over a support role while the evaluation is carried out. That is because a single requirement can be tested in several subsystems of the devices and could have several interpretations. The vendors should provide as much information as the evaluators needs in order to test all the possible requirements interpretations.

D. Compatibility of CC and IEC 62443

IEC 62443-4-1 SM-9 allows to integrate externally provided components that are certified to a similar security standard. From this, as well previous EDSA practice [20], and from mapping of CC assurance to IEC 62443-4-2 functional requirements [21], as well as from that most IEC 62443-4-1 activities are matched by a CC counterpart, we concluded that the separation kernel's CC certification allows for its use as subcomponent of a product under IEC 62443 certification.

VII. ACKNOWLEDGMENT

This work is part of the certMILS project under grant agreement No. 731456, funded by the European Union's Horizon 2020 research and innovation programme.

VIII. BIBLIOGRAPHY

[1] S. Tverdyshev, H. Blasum, B. Langenstein, J. Maebe, B. De Sutter, B. Leconte, B. Triquet, K. Müller, M. Paulitsch, A. Söding-Freiherr von Blomberg and A. Tillequin, "MILS Architecture," 2013. [Online]. Available: https://doi.org/10.5281/zenodo.45164.

[2] A. Hohenegger, "Security Certification of Cyber Physical Systems for Critical Infrastructure based on the Compositional MILS Architecture," in *Unpublished manuscript*, 2021.

[3] Common Criteria Sponsoring Organizations, "Common Criteria for Information Technology Security Evaluation. Version 3.1, revision 5," April 2017. [Online]. Available: http://www.commoncriteriaportal.org/cc/.

[4] A. Hohenegger, "Die Common Criteria und IEC-62443," in *Deutscher IT-Sicherheitskongress*, 2019.

[5] CENELEC, prTS 50701: Railway applications – Cybersecurity, CLC/FprTS 50701, 67491, vote for ts/tr, CLC/TC 9X, 2021-04-02, N, EN., 2021.

[6] International Electrotechnical Commission (IEC), "IEC 62443-4-1: Security for industrial automation and control systems - Part 4-1: Secure product development life-cycle requirements," 2018. [Online]. Available: http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx.

[7] International Electrotechnical Commission (IEC), "IEC 62443-4-2: Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components," 2019. [Online]. Available: http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx.

[8] IEC Systemof Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE System), "Rules of Procedure –CB Scheme of the IECEE for Mutual Recognition of Test Certificates for Electrotechnical Equipment and Components (CB Scheme) and its related services:Statement of Test Results - Energy Efficiency Testing Service (E3)Global Motor Energy Efficiency (GMEE) Program Industrial Cyber Security Program," p. 21, 2019.

[9] ISA Security Compliance Institute (ISCI), "ISASecure - IEC 62443 Conformance Certification - Official Site," 2020. [Online]. Available: https://www.isasecure.org/en-US/.

[10] exida.com LLC, "exida - IEC 62443 Cybersecurity Certification," 2020. [Online]. Available: https://www.exida.com/Certification/IEC62443-Cyber-Cert.

[11] K. Shankar and H. Kurth, "Certifying open source - the Linux experience," *IEEE Security and Privacy Magazine,* vol. 2, no. 6, pp. 28-33, November 2004.

[12] L. Bass, R. Kazman and P. Clements, Software Architecture in Practice, 3rd ed., 2012.

[13] BSI, "PikeOS Separation Kernal CC Certification Report," [Online]. Available: https://www.commoncriteriaportal.org/files/epfiles/1041a_pdf.pdf. [Accessed 28 June 2019].

[14] M. Paulitsch, H. Ruess and M. Sorea, "Non-functional Avionics Requirements," in *ISoLA*, 2008.

[15] J. Prochazka, P. Novobilsky, D. Prochazkova and T. Kertis, "Certification Cycles of Train Cyber Gateway," in *Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference (ESREL2020 PSAM15). No. 3728. ISBN 978-981-14-8593-0.*, 2020.

[16] exida.com LLC, "Comparing the IEC 62443 Software Engineering Process to IEC 61508: Where Do They Overlap?," 2020. [Online]. Available: https://www.exida.com/blog/comparing-the-iec-62443-software-engineering-process-to-iec-61508.

[17] ENISA, "Cybersecurity certification: EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS, V1.0, 01/07/2020," 2020. [Online]. Available: https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme/at_download/fullReport.

[18] J. E. Rico, H. Kurth, A. Hohenegger, A. Ortega, H. Blasum, S. Tverdyshev and M. Hager, "Base MILS Platform Protection Profile," May 2018. [Online]. Available: https://zenodo.org/record/2586499.

[19] A. Ortega, H. Kurth, A. Hohenegger, B. Caracuel, J. E. Rico, L. Garcia, H. Blasum and S. Tverdyshev, "MILS Platform PP Modules," May 2018. [Online]. Available: https://zenodo.org/record/2586507.

[20] ISA Security Compliance Institute, "SDLA-312 Security Development Lifecycle Assessment Version 3.0," 2014. [Online]. Available: http://www.isasecure.org/en-US/Certification/IEC-62443-SDLA-Certification.

[21] J. Rollo, H. Kurth, A. Hohenegger, A. Álvarez de Sotomayor, B. Caracuel, A. Ortega, S. Tverdyshev, H. Blasum and T. Kertis, "Guidelines to use and apply PP for all involved stakeholders," May 2018. [Online]. Available: https://zenodo.org/record/2586574.