
# D1.3: Compositional security certification methodology

| | |
|---|---|
| **Project number:** | 731456 |
| **Project acronym:** | certMILS |
| **Project title:** | Compositional security certification for medium to high-assurance COTS-based systems in environments with emerging threats |
| **Start date of the project:** | 1st January, 2017 |
| **Duration:** | 48 months |
| **Programme:** | H2020-DS-LEIT-2016 |

| | |
|---|---|
| **Deliverable type:** | Report |
| **Deliverable reference number:** | DS-01-731456/ D1.3/ 1.0 |
| **Work package contributing to the deliverable:** | WP 1 |
| **Due date:** | March 2018 |
| **Actual submission date:** | 26th March, 2018 |

| | |
|---|---|
| **Responsible organisation:** | Epoche and Espri |
| **Editor:** | Jose Emilio Rico |
| **Dissemination level:** | PU |
| **Revision:** | 1.0 |

| | |
|---|---|
| **Abstract:** | This document describes the methodology for compositional security certification. The approach allows carrying out lightweight evaluations of composed products with components previously certified which can be patched during their life cycle. The methodology focuses on maintaining the certification as much efficient as possible. |
| **Keywords:** | Compositional assurance, MILS, maintenance, certification methodology |

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 731456.

**Editor**

José Emilio Rico (E&E)

**Contributors**(ordered according to beneficiary numbers)

Miguel Bañón, Jose Emilio Rico, Álvaro Ortega (E&E)

Reinhard Hametner (THA)

Holger Blasum (SYSGO)

Michal Hager (EZU)

## Disclaimer

# Executive Summary

The compositional security certification methodology as presented in this document is the certification approach to be used in the scope of MILS security evaluations and certifications. The approach also provides means to integrate/compose compliant and certified components.

It briefly presents the different options for certification regarding the structure of the composition, including specific information covering Common Criteria and IEC 62443.

Concrete requirements for developers and methodology for evaluators is given so that the evaluation and certification process is supported through the use of this document, in addition to the requirements and methodology existent for both Common Criteria and IEC 62443.

An assurance continuity approach is followed in order to allow the certificate maintenance remain while analyzing the patch management carried out by developers to their composite products.

# Contents

# List of Figures



# List of Tables

# Chapter 1 Introduction

A usual desire when thinking on composition is that it maintains the level of assurance of underlying building blocks. Another good property would be to have constant assurance as the systems is maintained.

We can approach their achievements by constructing a methodology based in the composition certification while guaranteeing the assurance continuity during a reasonable timing by analyzing the patching development process.

The methodology asserts that if some assurance in the development process of the post-certificate patches has been checked, the composition should not lose the product certificate condition as a result of an upgrade.

This composite evaluation methodology is not based on any preconceived evaluation assurance level beyond the assurance profile applied in the evaluation of the composed products. The assurance of the composite evaluation in respect to the assurance continuity depends on the user risk analysis when using upgraded compositions originally certified following this methodology.

# Chapter 2 Compositional certification overview

## 2.1 Composition life cycle

The generic lifecycle of the composition comprises the components selection and composition certification.

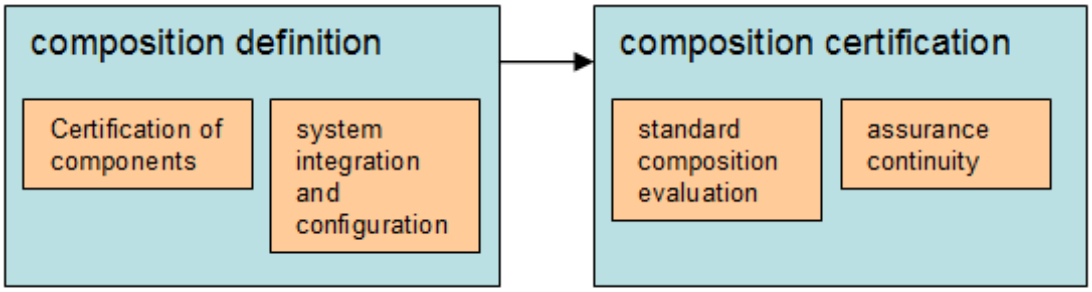


Figure 1: Composition life cycle

### *2.1.1 Composition definition overview*

The architecture of the MILS platform can be considered as a composition. The architecture composition supposes the existence of an extended base component and a set of additional components called applications, using the security functions provided by the extended base component.

The security requirements exhibited by the extended base component shall be based on a minimal base MILS Platform, which can be used either as a stand-alone, or including additional extension packages that include additional security functionality.

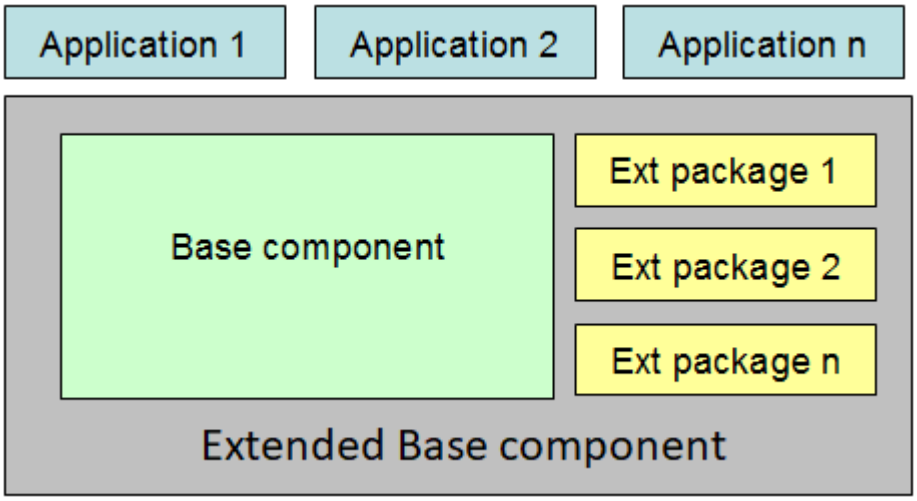


Figure 2: Composition structure

As an example, the components used to build the composition could be an OS separation kernel, extension packages and applications. These applications will use security functions provided by the OS and extension packages to achieve their security objectives.

### *2.1.2 Composition certification overview*

The composition shall address a previous integration and configuration phases to progress the composition to an evaluation readiness status.

The composition certification methodology will include the standard evaluation plus some additional activities oriented to the assurance continuity.

To guarantee the validity of the certificate of an already certified but upgraded composition during a reasonable timing, additional assurance activities have been extended for the patches management. Patching is considered always as an improvement of the products fixing known security bugs and therefore, requirements to this process are developed to guarantee that the patches are good enough to be tested by the developers, not only for their own functionality but also to avoid collateral effects.

A categorisation of the types of changes and an impact analysis will be required to the developer.

# Chapter 3 Composition definition

The MILS platform architecture can be decomposed in the following abstract levels:

- the base component and possible extension packages.
- and a set of additional components called applications, using security functions and properties provided by the base component.

## 3.1 Type of composition

The MILS approach allows two composition strategies:

- T-composition: the composition of the MILS platform with the applications running on the MILS platform.

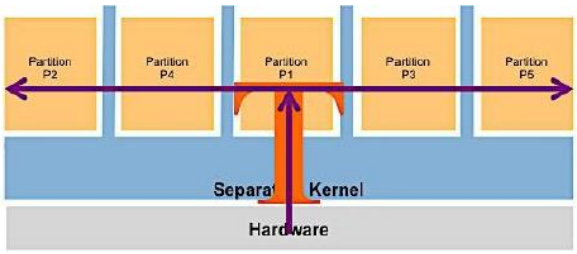


Figure 3: T-Composition

- I-composition: the composition that makes up the MILS platform itself, using COTS hardware.

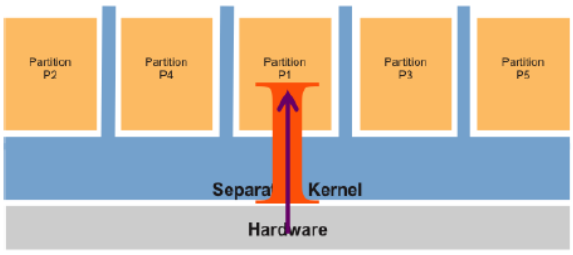


Figure 4: I-Composition

## 3.2 Certification of applications

For the applications, two scenarios may be given for the composition certification:

- The application has already been certified with a standard evaluation. For example, following with the example of the OS, the underlying OS separation kernel security features are included as assumptions in the security problem definition of the applications security targets.
- The application will be evaluated in the context of the composition.

# Chapter 4 Composition certification

## 4.1 CC composition certification

### *4.1.1 Certification of the base component and extension packages*

A modular Protection Profile is used to evaluate products with security targets according to PP configurations, which consist of a base Protection Profile and zero or more PP modules.

The evaluation of the base component and possible extension packages requires the development of an ST according to the PP configuration consisting in the base MILS Platform Protection Profile [D21] and the possible modular PPs for the interested extension packages.

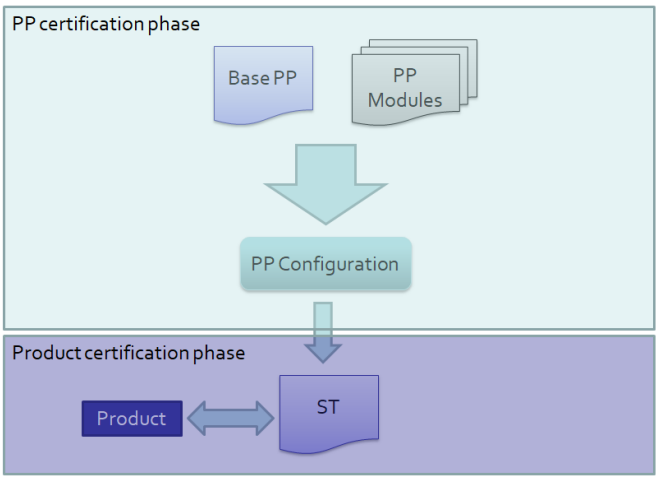


Figure 5: PP and Product certification phases

### *4.1.2 Applications composable features*

The key aspect to be considered when building a composition formed by one or more applications and the base component is the clear identification of the base component security features that the applications will use.

If no security claims can be mapped to the base component evaluated features other than isolation between partitions, and there is only a single application, the evaluation of a single application will be equivalent to that of a monolithic application with full control of the HW.

On the other hand, if instead of only one application, the composition is formed by the base component plus two or more applications, such composition shall be accurately defined so that it is clear how each part of the composition interacts with the others, and how the security features offered by all of them remain architecturally secure, available and trusted.

For that purpose, two certification approaches (CPE and ACO, presented in next subsection) can be followed depending on the suitability for each composition scenario.

Some examples of these composable features in the context of the OS separation kernel postulation may be:

- Fault Tolerance. A control application is replicated on multiple partitions. Information flow between them is allowed for the implementation of a voting system for fault tolerance. Because of the kernel separation properties, if an application crashes or gets frozen, this does not affect the others.

- Trusted Updates for applications where the integrity of the update is checked in a specific partition before swiping it to the target partition.

### *4.1.3 Composite product evaluation*

When the composition system is defined, we can address its evaluation according to the following scenarios:

1. All the components are certified.
2. The composition consists of an evaluated base component with unevaluated component.

Depending on the scenario, it could be better to follow an ACO [CC3] evaluation if we are in scenario 1 or to follow a CPE [CC5] approach if we are scenario 2.

The evaluation shall include also the extended package (ALC_PAT) for assurance continuity.

#### *4.1.3.1 CPE*

In this composition scenario where the application will be evaluated in the context of the composition, the CPE [CC5] shall be applied.

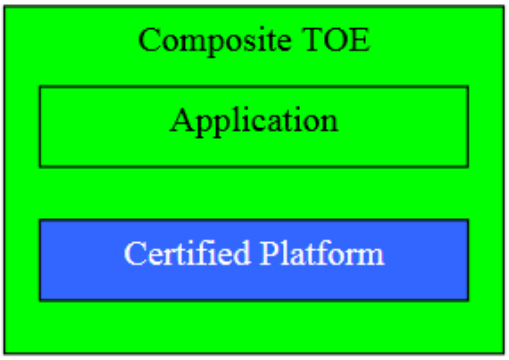


Figure 6: CPE

One of CPE's main objectives is to enable installing one or several applications onto an already certified platform in order to reduce the evaluation effort while keeping a high level of confidence. To this end, CPE provides rules and guidance for a transfer of knowledge between platform and application supplier and for a reuse of existing evaluation evidence.

#### *4.1.3.2 ACO*

In this composition scenario where the application has already been certified, the ACO [CC3] shall be applied.

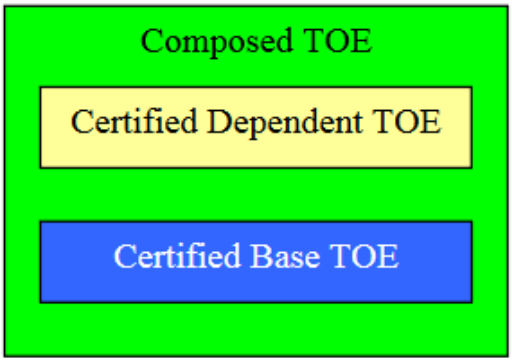


Figure 7: ACO

The ACO's main objective is to enable the certification of a composition of certified parts by examination and testing of the interfaces between the components, supported by examination of the design of the components and the conduct of vulnerability analysis.

### *4.1.4 Extended package for assurance continuity*

Maintenance refers to the process undertaken by the developer in order to demonstrate that the changes implemented do not adversely affect the assurance baseline of the composition.

The maintenance of the composition certificate is based in the analysis of the patches generation process.

Then, in addition to the proper CC activities associated to ACO/CPE, the following extended package must be covered in the certification process:

#### *4.1.4.1 Patching Management (ALC_PAT)*

**Objectives**

The objective of this family is to require the developer's patching management to have certain capabilities. These are meant to reduce the likelihood that functional error or vulnerabilities affects the certified composition and thus increasing the certificate validity period.

**Component leveling**

This family contains only one component.

**Application notes**

None

**ALC_PAT.1 Patching application**

Dependencies: No dependencies

Developer action elements:

**ALC_PAT.1.1D The developer shall analyse and apply patches to the parts of the composite TOE for which updates have been released.**

**ALC_PAT.1.2D The developer shall provide an Impact Analysis Report (IAR) recording the analysis of the impact of the changes to the certified composition.**

Content and presentation elements:

**ALC_PAT.1.1C The patch application procedures documentation shall describe the procedures used to track all the patches.**

**Associated evaluation methodology**

ALC_PAT.1-1 The evaluator ***shall check*** that the patch application procedures describe the procedures used to track the patches.

ALC_PAT.1-2 The evaluator ***shall check*** that the patch application procedures guarantee the application of all the patches associated to any part of the certified composition.

**ALC_PAT.1.2C The Impact Analysis Report (IAR) shall identify the component to which the patch has been applied.**

**Associated evaluation methodology**

ALC_PAT.1-3 The evaluator ***shall check*** that the IAR identifies the component to which the patch has been applied.

**ALC_PAT.1.3C** **The Impact Analysis Report (IAR) shall include a rationale indicating how the patch impact the security aspects of the certified composition.**

> **Associated evaluation methodology**
>
> ALC_PAT.1-4 The evaluator ***shall check*** that the IAR includes a rationale indicating how the patch impacts the security aspects of the certified composition.
>
> ALC_PAT.1-5 The evaluator ***shall check*** that the rationale provided is complete and clear enough to allow identify how the security aspects of the certified composition are affected.

**ALC_PAT.1.4C** **The Impact Analysis Report (IAR) shall summarize the additional security functionality the patch adds to the composite TOE.**

> **Associated evaluation methodology**
>
> ALC_PAT.1-6 The evaluator ***shall check*** that the summary is clear enough to allow identifying which security functionality is included and how this functionality affects the certified composition.
>
> If no additional security functionality is included in the patch, this work unit is not applicable.

Evaluator actions elements:

**ALC_PAT.1.1E** **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.**

## 4.2 IEC 62443 composition certification

In this section, as it will be needed below, we first discuss the general (composition-independent) configurability of IEC 62443 certification (Section 4.2.1), the applied maturity model (Section 4.2.2), then we describe applicable standards and scenarios (Section 4.2.3), followed by a discussion of process assessment specifications (Section 4.2.4) and product assessment specifics (Section 4.2.5), with the focus on a composition context.

The concept of IEC 62443 certification described below is based on Industrial Cyber Security Program under the IECEE system. The IEC System for Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE) is a multilateral certification system based on IEC International Standards. The principle of mutual recognition (reciprocal acceptance) of test results to obtain certification or approval at national levels around the world is applied. The System is the operator of the very successful IECEE CB Scheme, a one-stop shop that offers the potential of one test and one certification, recognized internationally. Moreover, the system is accessible to anyone anywhere, including in non-IEC member countries.

The certification scheme was designed by CMC Task Force Cyber Security under the IECEE and presents a unique approach for conformity assessment to IEC 62443 series of standards and for conformity assessments in the area of cyber security generally.

### *4.2.1 Configurability*

The most important feature and distinction of the IECEE Industrial Cyber Security Program [OD2061] is configurability. Configurability means that the applicant chooses the requirements that will be assessed, therefore he creates the scope of the assessment. That is done based on product/process specifications, risk analysis and/or final user requirements. Requirements of the selected standard that were not chosen will be assessed as "*not applicable*".

Because of this new approach, the certificates also have few specifics. Instead of demonstration of conformity to the full standard, it shows *Requirements assessed / Total Requirements* ratio. "*Requirements assessed"* represents a number of requirements that were successfully assessed. "*Total Requirements"* represents a total number of requirements in the highest organizational level of selected IEC 62443 standard. Those levels are as follows:

- *Summary Levels* - defined in IEC 62443-2-4
- *Practices* - defined in IEC 62443-4-1
- *Foundational Requirements* - defined in IEC 62443-3-3 and 62443-4-2

The example for IEC 62443-4-1 capability (*Practice*):

**SR (4/5)**

means that there are 5 requirements in Practice 2 (Specification of security requirements) and 4 of them were met.

### *4.2.2 Maturity model*

The applicant also chooses a maturity level for each requirement. Maturity levels with description relevant for product suppliers (manufacturers) and their development processes are described in the table below.

| Level | Description |
|---|---|
| **1 (Initial)** | Product supplier (manufacturer) is developing products in an ad-hoc manner and without a documented process. |
| **2 (Managed)** | Product (manufacturer) has the capability to develop products according to written policies and procedures describing the secure development lifecycle (including objectives). Product manufacturer also has evidence to show that personnel have the expertise, are trained and/or are capable of following the written procedures.<br>Development practices are repeatable, even during times of stress. When these practices are in place, their execution will be performed and managed according to their documented plans. |
| **3 (Defined /Practiced)** | A development process at Level 3 is a Level 2 development process that the product supplier (manufacturer) has practiced for an concrete product at least once.<br>The performance of a Level 3 development process can be shown to be repeatable across the product supplier's organization. |
| **4 (Improving)** | The product manufacturer (manufacturer) demonstrate continuous improvement, such as more effective procedures. This results in a security program that improves the development process through technological/procedural/management changes. |

Table 1: Maturity model

### *4.2.3 Applicable standards and scenarios*

As already identified in the D1.1 deliverable [D11], the most suitable standards from IEC 62443 series for the certMILS project and it´s compositional approach are:

- IEC 62443-4-1 Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements and
- IEC 62443-4-2 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components

The IEC 62443 series of standards generally specify requirements for security capabilities. These capabilities may be technical capabilities (security mechanisms) or process capabilities (human procedures). IEC 62443 conformance assessment consists of the evaluation of an applicant's security capabilities that it uses to develop, integrate and/or maintain specific products or solutions. Two evaluations can be conducted:

1) To evaluate an applicant's ability to provide IEC 62443 compliant security capabilities. This assessment focuses on evidence that supports the Applicant's submittal. This submittal contains the specific requirements and the processes used to implement the security capabilities for which they are requesting to be assessed.
2) To evaluate that these capabilities have been applied to:
   a) a specific product or
   b) a specific solution.

This creates two possible scenarios for certification:

- Scenario 1 – Capability Assessment: An assessment of a set of capabilities typically described in a plan or set of policies / procedures
- Scenario 2 – Application of Capabilities Assessment: Use of a Scenario 1 capability for a specific product or solution

When applied to the specific standards of IEC 62443 series applicable for certMILS project, the concrete scenarios are as follows:

- IEC 62443-4-1
  - Process Capability Assessment
  - Product Application Capability Assessment
- IEC 62443-4-2
  - Product Capability Assessment

They are described more into detail in the following subsections (4.2.4 and 4.2.5).

### 4.2.4 Process assessment

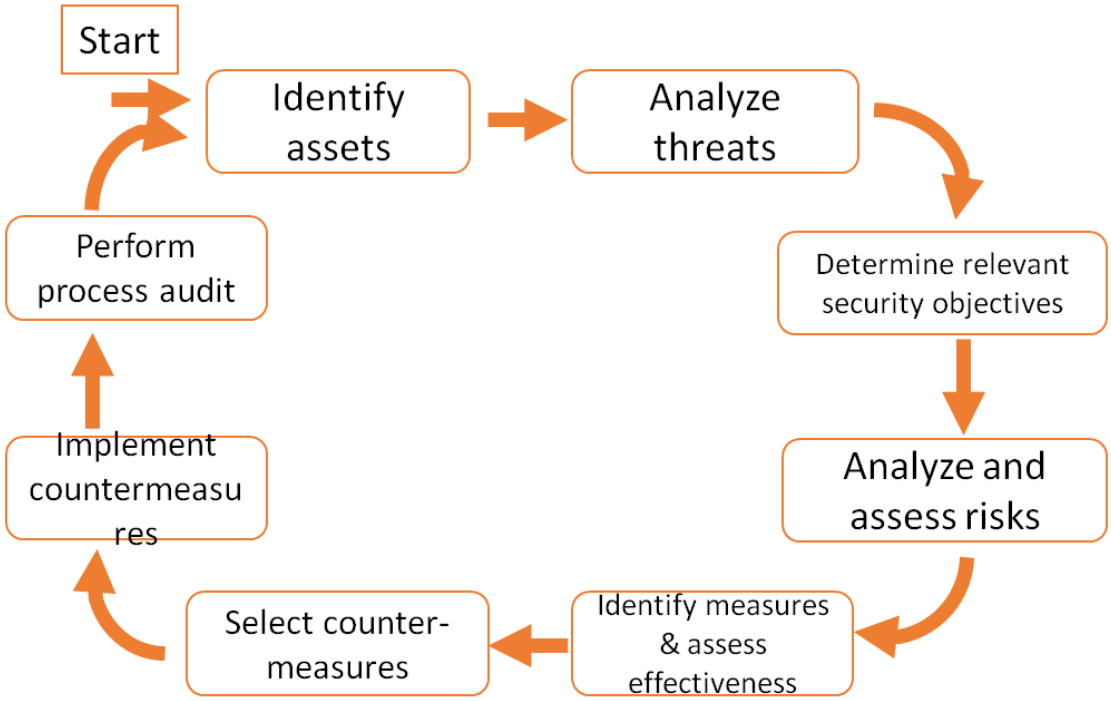


Figure 8: Security lifecycle, based on [IEC62443-1-1, Figure 5]

As shown in Figure 8, IEC 62443 suggests a lifecyle with continuous improvement, which is adopted from [VDIVDE2182].

This lifecycle shall exist at various product life cycle stages, at the level of product supplier, system integrator, and service provider [IEC62443-1-1, Figure 6], as depicted in Figure 9. What is important to note is that the lifecycles are continuous and chained together.

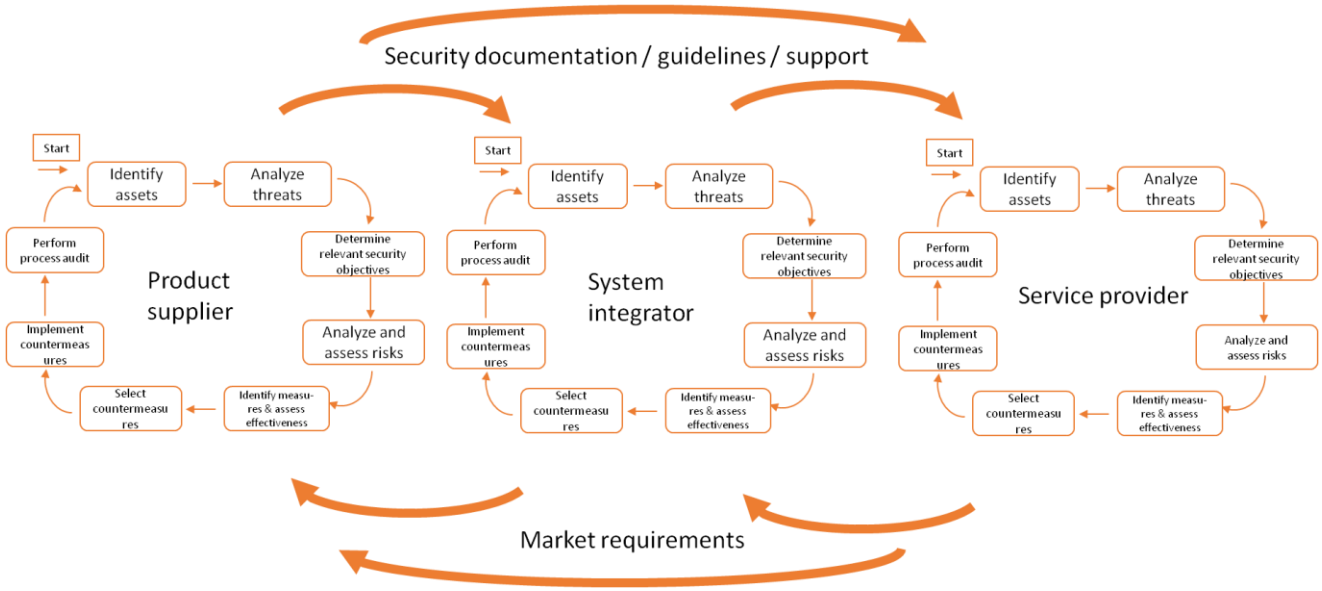


Figure 9: View of chained security lifecycles of component producers, integrators, and operators based on [IEC62443-1-1, Figure 6] and [VDE0831-104, Figure 5].

Where the main focus lies on the secure development lifecycle (SDL) of a product supplier (depicted is the left-most circle in Figure 9), the main interest should be for IEC 62443-4-1 and its

requirements. The requirements are focusing on security requirements definition, secure design, secure implementation, verification and validation, defect management, patch management and product end-of-life processes. These requirements can be applied to new or existing processes for developing, maintaining and retiring hardware, software or firmware for new or existing products.

### *Process assessment scenario for IEC 62443-4-1*

**IEC 62443-4-1 Process certification – Scenario 1**

Product supplier (manufacturer) has a development process for securely developing and supporting one or more products as required by IEC 62443-4-1. Following is the example for scenario 1 (the first of the two scenarios that were defined in Section 4.2.3):

- A product supplier has a formal development process, such as an ISO 9001 compliant process.
- The product developer has incorporated security into its product development processes according to 62443-4-1
- These security enhanced processes are formally documented.
- The product supplier submits an application for its development process to be assessed for conformance 62443-4-1.

## *4.2.5 Product assessment*

The product could be a system, subsystem or component such as network component, host device, embedded device and application. The candidate standards for product based scenarios are IEC 62443-4-2 and IEC 62443-4-1. There is a strong connection between IEC 62443-4-1 and IEC 62443-4-2 as IEC 62443-4-1 requirements require that security requirements for the product are identified (e.g. IEC 62443-4-2) and properly implemented in the product (with verification).

### *Product assessment scenarios*

**62443-4-1 - Product certification – Scenario 2**

Product supplier (manufacturer) has developed a product and supporting services (e.g. patching) using processes that were performed in accordance with requirements of IEC 62443-4-1. Following is the example:

- A product supplier has developed a product using 62443-4-1 processes.
- Those processes require the product supplier to apply security-related processes to all phases of development and support.
- The product supplier has generated documentation that shows it has followed it secure development processes for the product.
- This documentation shows traceability of security requirements through requirements definition, design and implementation, and testing.
- The product supplier submits an application to be assessed for conformance.

At the time of writing the scenarios for IEC 62443-4-2 are still in the preparation phase but they will follow the same principles described above. Expected time of completion is the end of 2018.

## 4.3 A pervasive compositional approach for use of a separation kernel

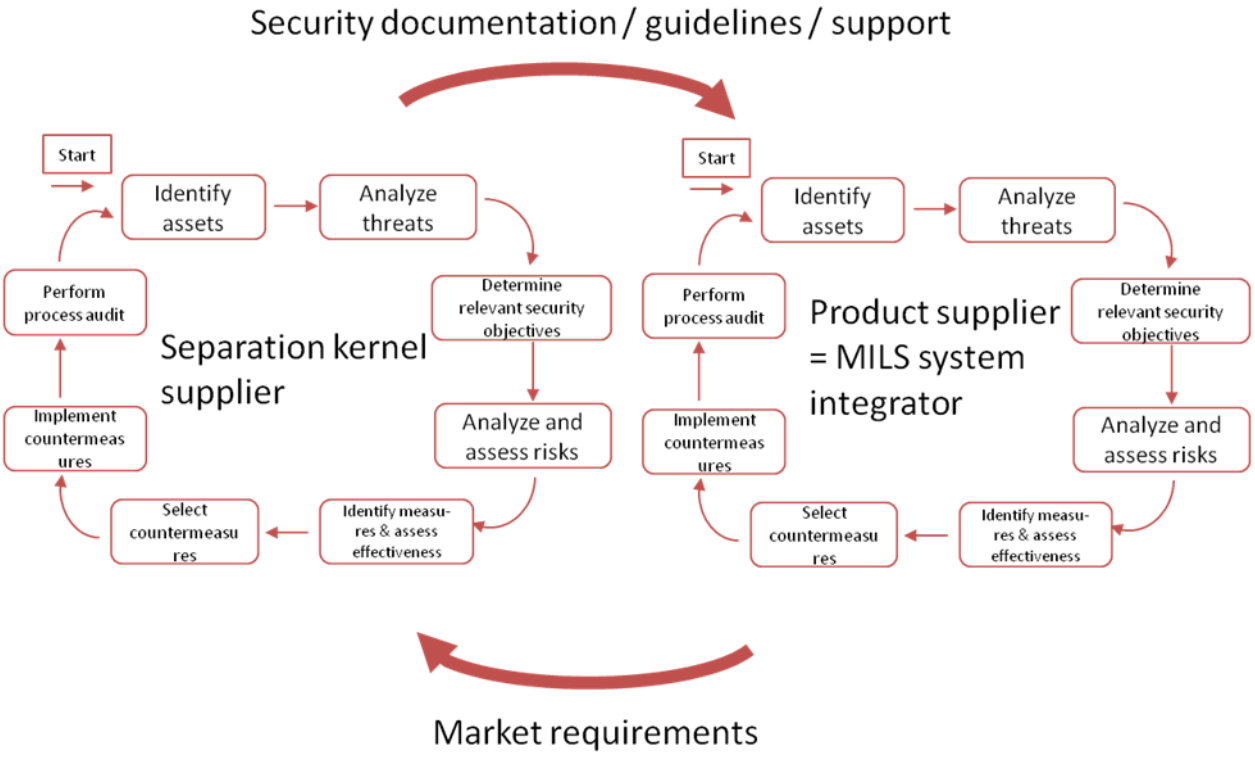


Figure 10: Chained security lifecycles in a MILS system

Note that the system integrators and service operators (i.e. railway companies, grid operators etc.) of Figure 9 (Section 4.2.4) are not directly represented in the certMILS prototypes. With regard to the actors in Figure 9, what we “only” have in the certMILS prototypes are in the railway, subway, and smart grid, are the product suppliers, which also occur left-most in Figure 9. However, certMILS also *does* have a notion of chained security lifecycles, once we add the separation kernel supplier, as shown in Figure 10.

In this section we discuss how the CC assurance gained for the separation kernel can be used to gain IEC 62443 assurance for the prototypes. We do this for IEC 62443-4-1 process requirements in Section 4.3.1 and for IEC 62443-4-2 functional requirements in Section 4.3.2. We also give a justification why this can be done for a separation kernel that has been certified according to CC in Section 4.3.3.

### *4.3.1 Process*

Using a separation kernel automatically enforces a partitioned architecture, which can be used to give credit to design assurance. As discussed in [D2.3, Section 4], the use of a separation kernel strongly supports adherence to the following process requirements of IEC 62443-4-1 (see Table 2).

| ID | Evidence supporting compliance with IEC 62443-4-1 requirements |
|---|---|
| SR-2 | This requirement is about threat models with clear trust boundaries. The trust boundaries in a separation kernel are the partitions. |
| SD-1 | This requirement states that a process shall be employed for developing and documenting a secure design that identifies and each exposed interface of the product, including physical and logical interfaces. Such documentation is provided by describing the domain separation in a separation kernel. |
| SD-2 | A process shall be employed for including multiple layers of defense where each layer provides additional defense mechanisms. Each layer should assume that the layer in front of it may be compromised. A separation kernel is a defense in depth. |
| SD-6 | This requirements asks to use least privilege (granting only the privileges to users/software necessary to perform intended operations); using proven secure components/designs where possible; economy of mechanism (striving for simple designs); using secure design patterns; attack surface reduction; and that all trust boundaries are documented as part of the design. All these activities are supported by the use of a separation kernel. |

Table 2: IEC 62443-4-1 Requirements fulfilled by a use of separation kernels

In a pervasive approach, one could use the set of process requirements indicated in Table 2 as a (small) configuration (for the concept of configurations see Section 4.2.1) for an initial IEC 62443-4-1 process certification, giving SR (1/5) and SD (3/6).

### *4.3.2 Product*

As discussed in Section 4.3.1 the use of a separation kernel strongly supports adherence to the IEC 62443-4-1 process requirements. It can further support the following component requirements defined in 62443-4-2 (see Table 3). Description of requirements is based on the draft of the standard as the final version of the standard has not yet been published.

| ID | Evidence supporting compliance with IEC 62443-4-2 requirements |
|---|---|
| CR 5.1 | Components shall support a segmented network as defined in ISA 62443-3-2, as needed, to support the broader network architecture based on logical segmentation and criticality. This is relevant for certMILS use cases that connect different networks to functionality. |
| CR 7.1 | Components shall provide the capability to maintain essential functions in a degraded mode during a DoS event. This is relevant for certMILS use cases where availability matters. |
| CR 7.2 | Components shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion. This is relevant for certMILS use cases where availability matters. |

Table 3: IEC 62443-4-2 Requirements that a separation kernel can help the prototypes with

Thus, in a pervasive approach, one could use the set of product requirements indicated in Table 2 as a (small) configuration (for the concept of configurations see Section 4.2.1) for an initial IEC 62443-4-2 product certification, giving CR 5 (1/3) and CR 7 (2/8).

### *4.3.3 Validity of separation kernel CC-certification for IEC 62443 prototypes*

In a world where resources were unlimited, the separation kernel would also have undergone a more broader 62443-4-X certification. However, as separation kernels are general purpose products, and not limited to industrial control systems, from a market perspective, for a separation

kernel vendor it is more meaningful to certify against CC. Hence we argue that the CC process requirements are sufficient for a separation kernel to be used as a component.

The most important argument why a CC certification is sufficient for a MILS separation kernel to be used in a CC context is that the core activity of the CC as well as of IEC 62443-4-1 is to do a threat analysis, based on the identification of assets, threats, adverse agents, security objectives and functional measures to achieve them. IEC 62443-1-1 explicitly has adopted a thread model based on the CC model [IEC-62443-1-1, Section 5, Figures 2 and 3]. This also can be seen in the chained lifecycle depicted in Figure 10.

In addition, with regards to lifecycle, even at moderate EAL levels CC bring in lifecycle assurance, which can be mapped to IEC 62443-4-1 (see Table 4).

| CC activity | IEC 62443 counterpart |
|---|---|
| Development (ADV) | IEC 62443-4-1 Practice 3 Secure by Design; Practice 4 Secure Implementation |
| Testing (ATE) | IEC 62443-4-1 Practice 5 Testing |
| Vulnerability analysis (AVA) | IEC 62443-4-1 SV-4 Penetration testing |
| Configuration management capabilities (ALC_CMC) | IEC 62443-1-1 Section 8 Lifecycle |
| Configuration management scope (ALC_CMS) | IEC 62443-1-1 Section 8 Lifecycle |
| Delivery (ALC_DEL) | IEC 62443-1-1 Section 8 Lifecycle |
| Development security (ALC_DVS) | IEC 62443-4-1 SM-7 Development environment security |
| Life-cycle definition (ALC_LCD) | IEC 62443-1-1 Section 8 Lifecycle |
| Flaw remediation (ALC_FLR) | IEC 62443-4-1 Practice 6 Security defect management |

Table 4: Mapping of CC activities to IEC 62443

The sufficiency of CC certification for operating systems is also indicated in IsaSecure's guideline for the application of IEC 62443-4-1, SDLA-312 [SDLA312, MIV-5 (Module Implementation & Verification)], suggests that "*If the product includes a Commercial off the Shelf (COTS) operating system, then the operating system shall either meet the requirements of this development phase or be certified to Common Criteria EAL 3 or higher or be certified to a comparable security standard, or compensating controls must be included in the product to ensure that security vulnerabilities in the operating system do not result in vulnerabilities above a certain severity level in the product.*" Similar, for the railway sector, VDE 0831-104 [VDE0831-104, p. 19] states for **compatible certifications** that "*it is assumed that in future railway signalling systems components with IT security tasks are usually purchased on the marked and not developed in-house. It is assumed that such components already have a certification compatible with IEC 62443. If this does not apply, after checking the requirements one also could accept other certificates or compare with a reference system*".

Therefore, we conclude that a CC certification of a separation kernel suffices for its use as subcomponent of a product under 62443-4-1/62443-4-2 certification.

# Chapter 5 Assurance Continuity

This section will include the definition of the assurance continuity process. It covers the methodology for the assurance continuity in terms of what is expected from the developer and what is to be performed by the evaluator.

## 5.1 Patch management

### *5.1.1 Patching system*

The patching system used by the developer must implement:

1. information gathering activities for patch management, including inventory of patchable system, supportability, product supplier relationship building, and evaluation and assessment of the existing environment.
2. project planning and implementation activities for patch management, including developing the business case, definition of roles and responsibilities, establishing a patch deployment infrastructure, and establishing a backup and restoration infrastructure.
3. procedures and policies for patch management, including monitoring for patches, patch evaluation, testing, patch deployment, and change management.
4. activities of operating a patch management system, including executing the procedure and policies, vulnerability awareness, outage scheduling, inventory maintenance, new device additions, reporting and key performance indicators (KPIs), and auditing and verification.

**EVALUATION METHODOLOGY: The evaluator must check and confirm that all these requirements are satisfied.**

### *5.1.2 Impact Analysis Report (IAR)*

The developer shall provide an Impact Analysis Report (IAR) recording the analysis of the impact of the changes to the certified composition.

Performing an impact analysis and the generation of the corresponding IAR procedures are defined in [CC6].

In addition to what is indicated in [CC6], it must also indicate, when applicable:

1. Component standard patches fixing internal Bugs that do not affect the external interfaces or the associated security functionality.
2. Component standard patches fixing internal Bugs that affect the external interfaces or the associated security functionality.
3. Patches adding security functionality
4. New application or base-component (e.g. platform) or extension package integration

**EVALUATION METHODOLOGY: The evaluator must check and confirm that all these requirements are satisfied.**

### *5.1.3 Developer Regression Testing*

According to the impact analysis, the developer shall execute regression testing on the updated TOE recording its results and making them accessible for the final user.

The developer test plan must include tests for each patch applied. The granularity of the tests must be at a level such that all the aspects of each patch are tested.

The test cases must detail the configuration used for the test, the prerequisites to be satisfied including ordering dependencies, test steps, expected results and actual results.

**EVALUATION METHODOLOGY: The evaluator must check that the developer test plan and report satisfies these requirements.**

**EVALUATION METHODOLOGY: The evaluator must confirm that the developer test plan is consistent with the patching system and with the Impact Analysis Report.**

### *5.1.4 Reusability of Base-component Evaluation Certificates*

In order to reuse existing component certificates, the evaluation of these components must be sufficiently up-to-date and remain valid at the time of the maintenance.

## 5.2 IEC 62443 Specifics

With regards to the IEC 62443 certification scheme (described in Section 4.2), an IEC 62443 certificate issued under the Industrial Cyber Security Program under the IECEE system does not have an expiration date. The scheme assumes that the assurance continuity is ensured by the IEC 62443 Process Requirements and it is a solely responsibility of the applicant (in this case the product supplier), who is driven by his customer requirements and the applicant´s product/process.

## 5.3 Pervasive compositional approach specifics

With regard to the pervasive approach (described Section 4.3), the separation kernel developer is to follow the CC assurance continuity approach and to notify the MILS system users (prototypes) with updates / guidance should security flaws that affect the MILS system security objectives, in the same way it is done for IEC 62443 process.

# Chapter 6 Summary and Conclusion

This document covers the compositional certification and evaluation methodology to be applied on products based on the MILS architecture. For that purpose, two certification standards have been covered and extended: CC and IEC 62443. The methodology is common in several phases for both CC and IEC 62443, but different approaches must be considered for fulfilling specific aspects of each standard, and such differences have been detailed in previous sections.

The MILS architecture concept makes the certification approach compositional. Such certification approach allows the certification of the composition of several already certified parts making the certification effort easier and less time-consuming.

Regarding the maintenance of the certification, an assurance continuity approach is considered based on the patching system the vendor must cover and satisfy after the certification.

# Chapter 7 List of Abbreviations

| Abbreviation | Translation |
|---|---|
| ACO | Common Criteria Composition Assurance Class |
| ALC | Common Criteria Life Cycle Assurance Class |
| CC | Common Criteria |
| CPE | Composite Product Evaluation |
| EAL | Evaluation Assurance Level |
| IAR | Impact Analysis Report |
| IEC | International Electrotechnical Commission |
| MILS | Multiple Independent Levels of Security |
| OS | Operating System |
| PP | Protection Profile |
| ST | Security Target |
| TOE | Target of Evaluation |

# Chapter 8 Bibliography

[CC1] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1, Revision 5. April 2017. CCMB-2017-04-001

[CC2] Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components.Version 3.1, Revision 5. April 2017. CCMB-2017-04-002

[CC3] Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components.Version 3.1, Revision 5. April 2017. CCMB-2017-04-003

[CC4] Common Criteria for Information Technology Security Evaluation. Evaluation Methodology.Version 3.1, Revision 5. April 2017. CCMB-2017-04-004

[CC5] Composite product evaluation for Smart Cards and similar devices. Version 1.2, April 2012. CCDB-2012-04-001

[CC6] Assurance Continuity: CCRA requirements. Version 2.1. June 2012.

[D11] certMILS Deliverable D1.1Regulative Baseline. Version 1.0 June 2017

[D21] certMILS Deliverable D2.1 Base MILS Platform Protection profile. Version 1.0 April 2018

[D23] certMILS Deliverable D2.3 Security Architecture Templates, Version 1.0, April 2018

[IEC62443-1-1] IEC 62443 Part 1 Section 1, Draft 6, Edit 4, March 2017

[IEC62443-4-1] IEC 62443 Part 4 Section 1, Draft 3, Edit 11, March 2016

[IEC62443-4-2] IEC 62443 Part 4 Section 2, Draft 4, Edit 1, January 2017

[OD2061] IECEE PUBLICATION, Industrial Cyber Security Program, Edition 1.0, 2016-11-28

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

[VDE0831-104] VDE 0831-104, Bahn-Signalanlagen, Elektronische Bahn-Signalanlagen - Part 104: Leitfaden für die IT-Sicherheit auf Grundlage IEC 62443 (Electric signalling systems for railways - Part 104: IT Security Guideline based on IEC 62443), October 2015

[VDIVDE2182] VDI/VDE Guideline 2182, IT-security for industrial automation, General model, January 2011