SYSGO
EMBEDDING INNOVATIONS

Security Certification Kit

Cc

Common Criteria

SYSGO & PikeOS

Security is different to Safety and this is especially true when it comes to testing and validation. While functional Safety requirements can be tested by observing the system's behaviour and comparing it to the input requirements, Security is about the absence of vulnerabilities.

As it is impossible to test a system against all possible input vectors, it seems that protection against all Cyber Security threats cannot be assured. However, systems may be tested against a representative set of penetration input vectors, merely hoping that no critical path has been overseen.

Content

1. Introduction

Security is different to Safety and this is especially true when it comes to testing and validation. While functional Safety requirements can be tested by observing the system's behaviour and comparing it to the input requirements, Security is about the absence of vulnerabilities.

As it is impossible to test a system against all possible input vectors, it seems that protection against all Cyber Security threats cannot be assured. Systems may be tested against a representative set of penetration input vectors, merely hoping that no critical path has been overseen.

However, there are standardized and consistent ways to evaluate a system and achieve Security certification. One of those, if not one of the most recognized standard, is the Common Criteria for Information Technology Security Evaluation (Common Criteria or CC). SYSGO has certified its PikeOS hypervisor according to the CC.

Nevertheless, an entire system can only be considered as secure after all critical parts have been evaluated. Evidently, one of the most critical parts is your application running on top of the PikeOS Hypervisor. That is why SYSGO's engineers have created the Security Certification Kit. It aids you in achieving the same level of Security for your application and entire system by applying the same rules of evaluation that were used during the certification of the PikeOS Hypervisor.

The Certification Kit comes with a Security manual, all required interface documents as well as the augmented Security Target (ST). This special version of the ST differs from the public one and has been augmented by requirements identification numbers (ids). These identifiers are essential when you are about to build up the complete system traceability.

The Certification Kit is completed by a periodical Security bulletin, certification support and services.

2. Baseline for the Security Certification Kit

- Most hard to fix Security flaws are caused by incorrect or violated architectural assumptions
- These assumptions are made early in the product's life cycle (see Figure 1)

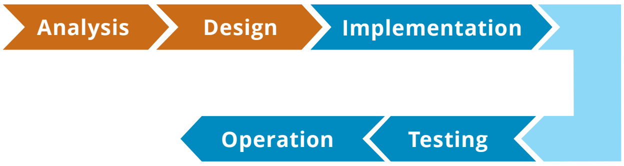

Figure 1: Scheme of a product life cycle

Examples for possible Mistakes:

- Not clearly defining the trust relationships within the system
- Semantic shift: Using non-confidential data (serial numbers, user names, ...) as a secret, e.g. as input to an encryption algorithm
- Relying on features of the underlying hardware/software layers that were not designed for Security
- Architectural Security flaws are difficult or infeasible to fix at a later point in the life cycle
- It is important that all necessary information is present at these critical early phases

When is a Security Certification Kit needed?

- Case 1: Provision of evidences to an authority or an end customer that PikeOS fulfills its SFR (Security Functional Requirements)
- Case 2: Development of a BSP and partially configure PikeOS to create a platform
- Case 3: Development of applications and configuration of a platform built on PikeOS and the relevant BSP

3. Certification Kit for Cyber Security (Common Criteria Evaluation)

For different architectures, such as x86 64-bit, ARMv8, or PowerPC, the product is aligned to fulfill basic customer requirements and artefacts needed for their certification projects, such as:

- Certification Kit user manual
- Augmented Security Target (ST)
- Common Criteria certificate
- Security manual for PikeOS
- Software high-level requirements documentation
- Interface documentation for all PikeOS components
- Stack analysis, timing analysis and partitioning analysis reports for PikeOS
- Traceability documentation

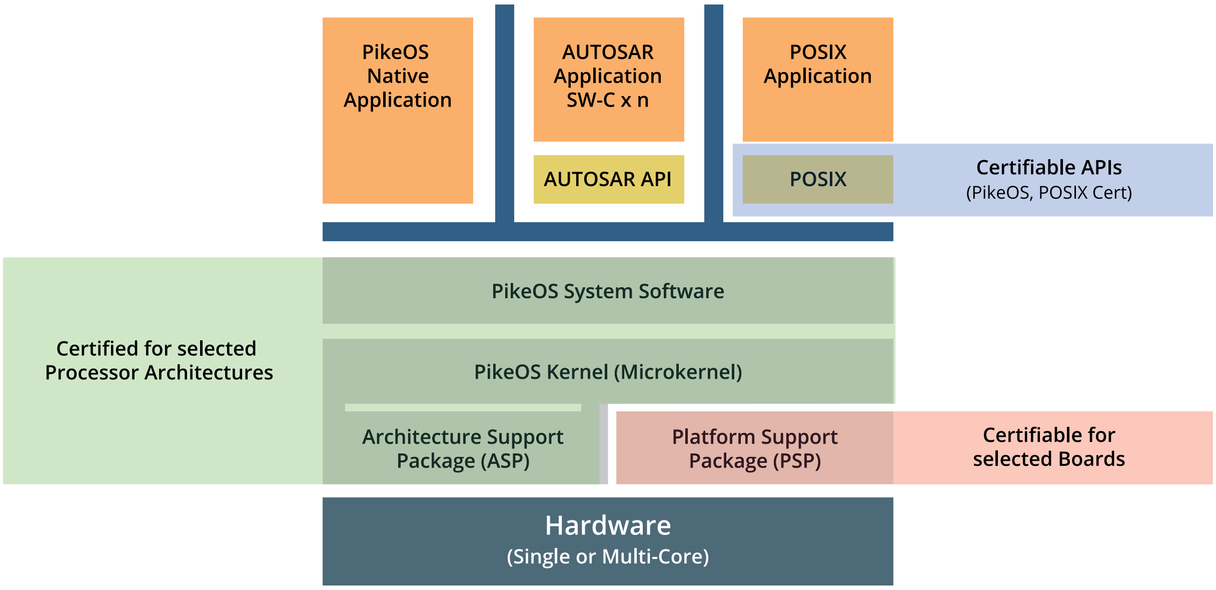
PikeOS Native Application
AUTOSAR Application SW-C x n
POSIX Application
AUTOSAR API
POSIX
Certifiable APIs
(PikeOS, POSIX Cert)
Certified for selected Processor Architectures
PikeOS System Software
PikeOS Kernel (Microkernel)
Architecture Support Package (ASP)
Platform Support Package (PSP)
Certifiable for selected Boards
Hardware
(Single or Multi-Core)

Figure 2: Certifiable and certified components in a running PikeOS System

4. SYSGO Certification Components

The Certification Kit is complemented with a certification services package. The main objective of this service is to establish communication and understanding between SYSGO, the customer and the certification authorities regarding the certification aspects throughout the software life cycle and to assist the customer in the certification process.

The coordination with the certification authorities is typically managed by the customer. Nevertheless, SYSGO has established a good partnership to the certification authorities due to successful past projects. Therefore, the attendance of SYSGO to audits and meetings with authorities is usual. SYSGO is open to provide detailed information about the developed products upon request.

The certification services included in the Security Certification Kit comprise one year access to the Security bulletin as well as 100 hours of consulting.

5. Highest Quality & Common Criteria Certification

As our products are used in the most critical environments and applications, SYSGO has strict in-house quality requirements in product development.

Our company processes are certified according to ISO 9001:2015 (Quality Management), and we achieved the certification against the DIN EN ISO / IEC 27001:2017 (Information Security Management).

Since 2022, the PikeOS Separation Kernel Version 5.1.3 is also certified according to Common Criteria EAL 5+.

6. Customer Benefits

SSM (Safety Security Manual) with generic Information about:

- Technical and personal prerequisites,
- Set-up procedures and
- Configuration guidance for the secure usage of PikeOS

Benefit: Avoid mistakes in the Security architecture when using PikeOS

Architecture-specific Safety Security Manual with Information about:

- Security impact and advice for usage of certain hardware features (e.g. hyper-threading),
- Hardware errata with Security impact
- Workarounds for errata, where possible

Benefit: Avoid Security issues on the level of the underlying hardware

Design Documentation (High-Level Requirements and Interface Requirements):

- Extensive PikeOS design documents

Benefit: Risk mitigation of basing your system architecture on possibly invalid assumptions about PikeOS

ALC_FLR.3 (Flaw Remediation):

- Security bulletins informing you about known vulnerabilities of components of your system (hardware or PikeOS)

Benefit: Ensuring a quick and adequate reaction on new Security threats

All product and service names mentioned are the trademarks of their resp. companies. National product specifications may vary. Data contained in this document serves informational purposes only and are subject to change without notice. SYSGO GmbH shall not be liable for errors or omissions with respect to the materials. Warranties are only set forth in the express warranty statements accompanying SYSGO products and services, if any.