Security Certification Kit

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

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 for short). 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.

CERTIFICATION KIT FOR CYBER SECURITY (COMMON CRITERIA EVALUATION)

For different architectures, such as x86 64-bit, ARMv8, or PowerPC, the product is aligned to fulfil 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

CERTIFIED COMPONENTS

The architecture of a PikeOS example system is shown in figure 2. The green sections are part of the PikeOS operating system and fully covered by each Certification Kit. The yellow certifiable APIs are ready for certification in the context of the particular project.

In addition, certification artefacts for some selected platform support packages are ready to use. Nonetheless, most certification projects will come along with customized hardware. In case the customer opts to develop and validate the required platform support package on its own, SYSGO provides the according tools.

SYSGO CERTIFICATION SERVICES

The Certification Kit is complemented with a certification services package. The main objective of this service is to

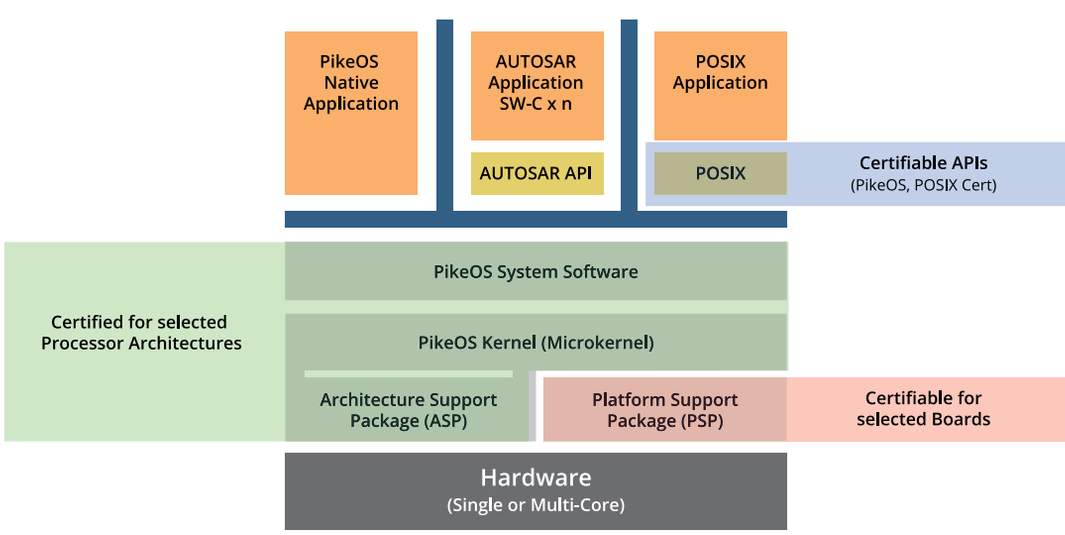

Figure 2: Certifiable and certified components in a running PikeOS System

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.

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 in 2016 we achieved the certification against ISO/IEC 27001:2013 (Information Security Management).
Since 2019 the PikeOS Separation Kernel Version 4.2.3 (build S5577) is also certified according to CC EAL3+.

SYSGO Headquarters
Phone +49 6136 9948 500
sales@sysgo.com

SYSGO France
Phone +33 1 30 09 12 70

SYSGO Czech Republic
Phone +420 222 138 111

www.sysgo.com