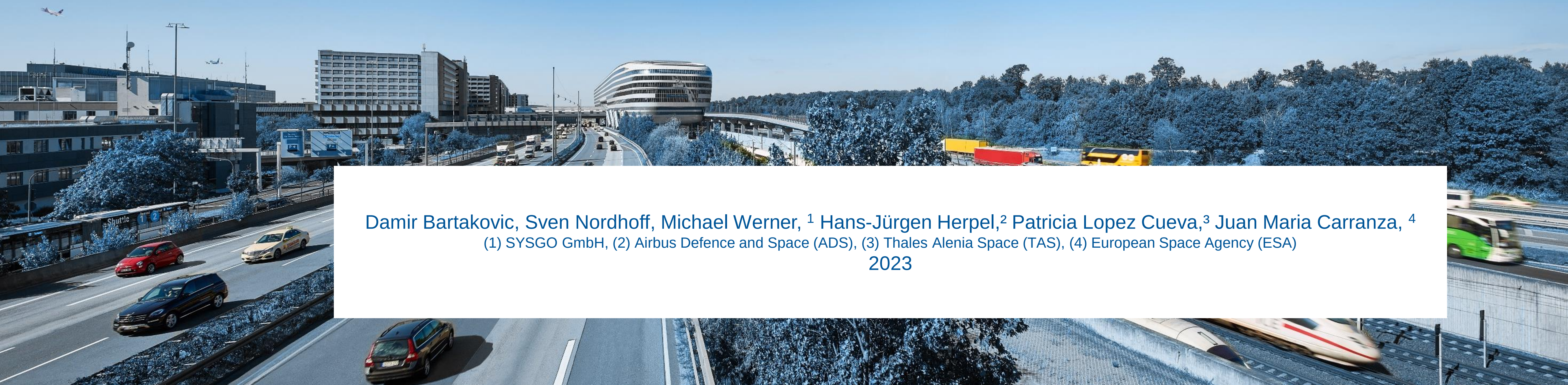
Copyright © SYSGO.

SYSGO
EMBEDDING INNOVATIONS

ESA CYBERSECURITY BY DESIGN FOR MIXED CRITICALITY EMBEDDED SYSTEMS

Damir Bartakovic, Sven Nordhoff, Michael Werner, [1] Hans-Jürgen Herpel,[2] Patricia Lopez Cueva,[3] Juan Maria Carranza, [4]
(1) SYSGO GmbH, (2) Airbus Defence and Space (ADS), (3) Thales Alenia Space (TAS), (4) European Space Agency (ESA)
2023



AGENDA

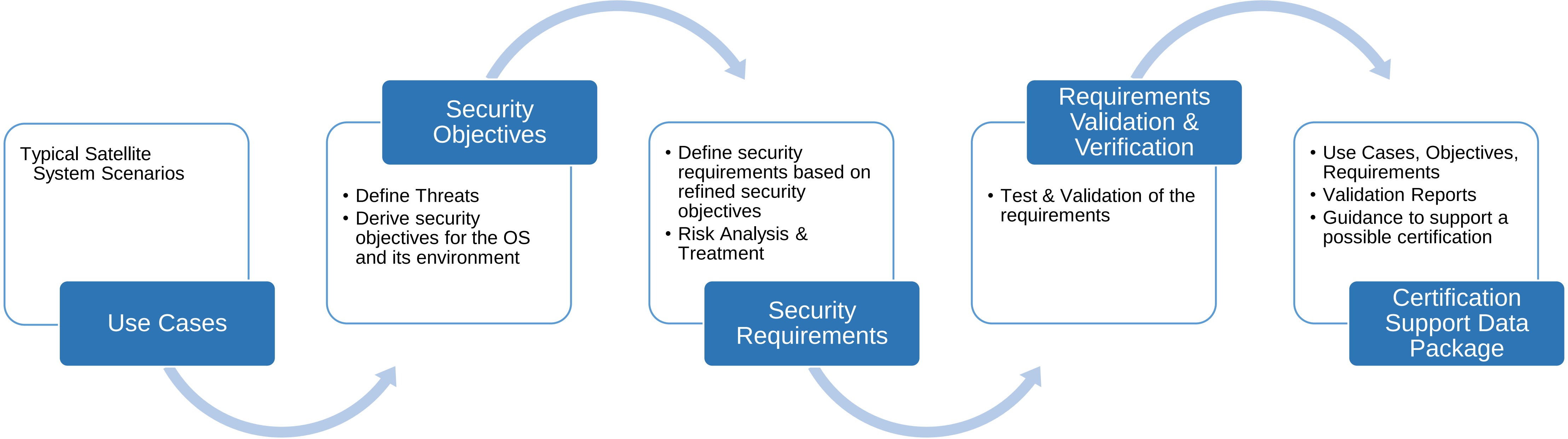
Project Overview
Security in Space, Study Overview, NG-ULTRA [1, 2, 3]

Project Synthesis

Next / Closing

ESA STUDY CYBERSECURITY BY DESIGN FOR MIXED CRITICALITY EMBEDDED SYSTEMS

- In a joint cooperation with ESA, Airbus, TAS and SYSGO the result of this study was the proof that the RTOS PikeOS for MPU offers properties and features that allow implementing secure applications with different security sensitivity for the R52 CPU Architecture (see next slide), which is running on the NG-ULTRA.



Use Cases

Typical Satellite System Scenarios

Security Objectives

- Define Threats
- Derive security objectives for the OS and its environment

Security Requirements

- Define security requirements based on refined security objectives
- Risk Analysis & Treatment

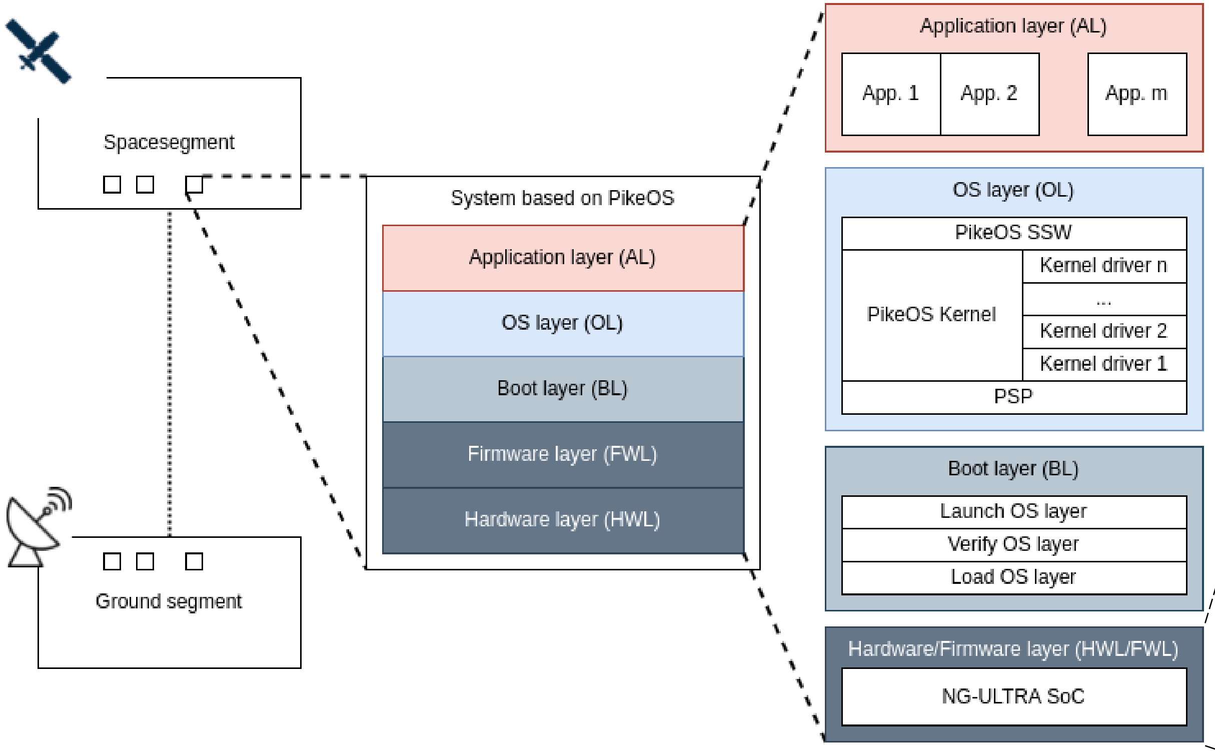
Requirements Validation & Verification

- Test & Validation of the requirements

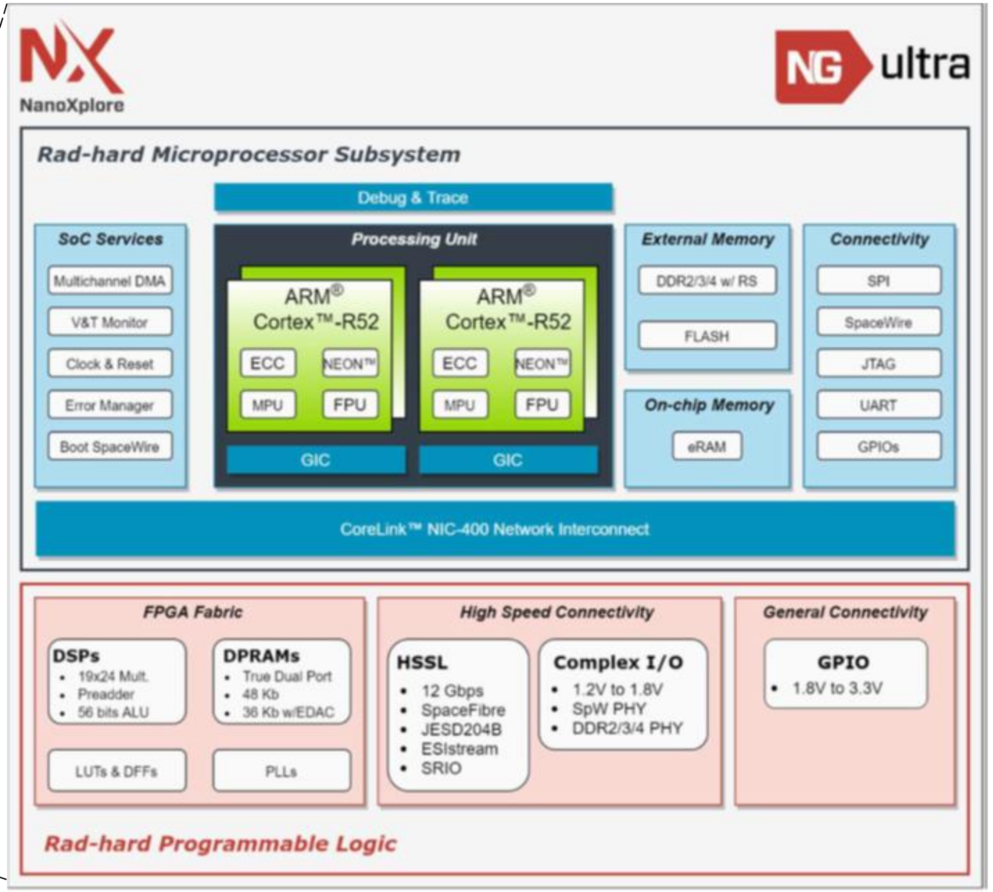
Certification Support Data Package

- Use Cases, Objectives, Requirements
- Validation Reports
- Guidance to support a possible certification

NG-ULTRA & PIKEOS FOR MPU



Example System based on PikeOS for MPU Architecture



NOTE: For the study, the NG-Ultra HW was replaced by a simulation environment based on FVP (HW was not available at ESA)

[1] https://dahlia-h2020.eu/ (**D**eep sub-micron microprocessor for sp**A**ce rad-Hard app**LI**cation **A**sic)

[2] https://eurospace.org/dasia-conference-aspx/ - Programme : NG-Ultra: a system-on-chip suiting the upcoming space missions (TAS, May 17th 2022)

[3] https://www.sysgo.com/pikeos-for-mpu

USAGE SCENARIOS & USE CASES

In cooperation with **ADS** and **TAS** the typical satellite mission usage scenarios e.g.:

- Earth Observation
- Satellite Navigation
- Satellite Telecommunications
- Deep Space

and use cases deemed relevant for security were analyzed and mapped e.g.:

- Protection of the OS layer from applications, and applications from other applications.
- Protection of the communication to and from external systems.
- Access Control

PROJECT SYNTHESIS

- We initiated the **Common Criteria** (ISO/IEC 15408) like analysis for **PikeOS for MPU**
- We ported the PikeOS (MMU) security target (ST) test suite to MPU and to the new architecture for ARM Cortex R52.
  - The test suite was successfully executed and delivered with 100% Coverage.
- We mapped the PikeOS for MPU security properties to the System as a whole, validated on several use cases.
  - All the testing performed in this project are security related, and only security related, as it was the focus
  - Correspond to about 10% of the existing PikeOS requirements

CERTIFICATION SUPPORT PACKAGE

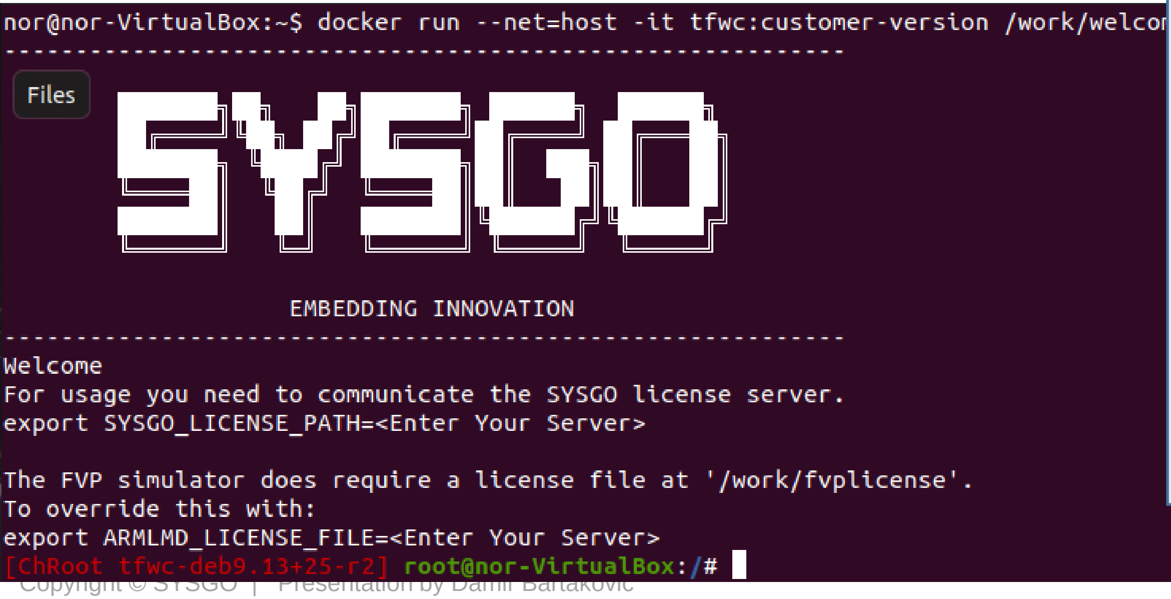
The package shows which documents and artifacts must be produced, and what evidence must be collected along the lifecycle of the project based on proven standards [ECSS], [ED-203A], [DO-356A] and especially for cyber-security [CC].

We recommend following:

- Common Criteria, as used in this study, or a similar approach can be the security standard.
- Certifying the RTOS and SBRTOS (**S**ystem **B**ased on the **RTOS**) would preferably be done separately.
- Lower-level separation security objectives should be provided and validated by the RTOS.
- SBRTOS certification shall specify, high-level system security objectives including analysis of security risks and security risk treatments.

DOCKER IMAGE TO RE-EXECUTE VALIDATION

- A full-functional test-environment was provided including the
  - SYSGO Test Framework (TFW)
  - The target as ARM FVP R52 (Simulation)
  - PikeOS for MPU
- Single tests or the complete test run can be reproduced
- An introduction with a live demo to use it was conducted.



```
nor@nor-VirtualBox:~$ docker run --net=host -it tfwc:customer-version /work/welco
-----------------------------------------------------------

                    EMBEDDING INNOVATION
-----------------------------------------------------------
Welcome
For usage you need to communicate the SYSGO license server.
export SYSGO_LICENSE_PATH=<Enter Your Server>

The FVP simulator does require a license file at '/work/fvplicense'.
To override this with:
export ARMLMD_LICENSE_FILE=<Enter Your Server>
[ChRoot tfwc-deb9.13+25-r2] root@nor-VirtualBox:/#
```

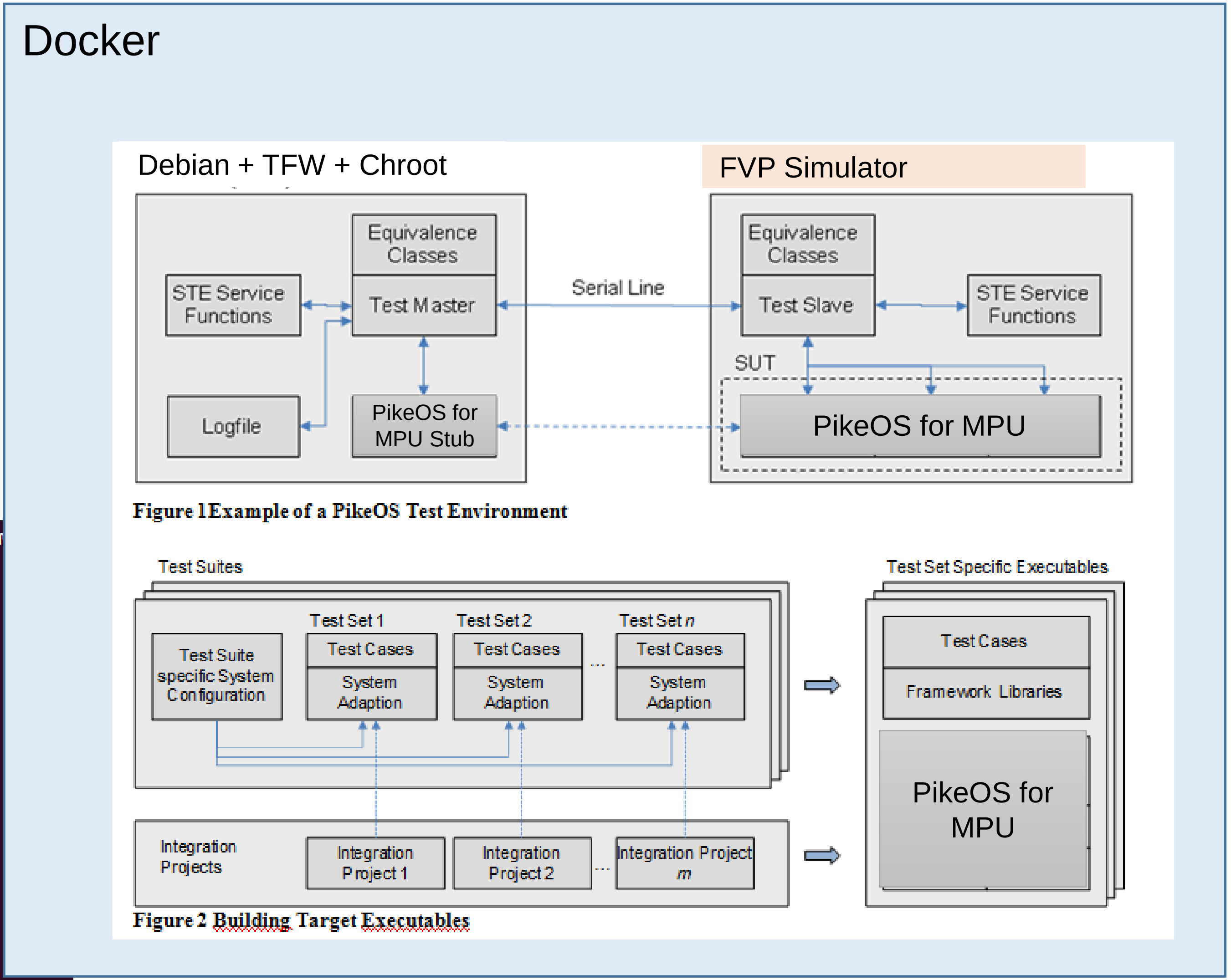


Figure 1Example of a PikeOS Test Environment

Figure 2 Building Target Executables

VALIDATION AND VERIFICATION INFRASTRUCTURE

SYSGO Test Framework (TFW)

- **XML based test description** for analysis, inspection, normal and robustness test cases
- Generation of **Camera-ready** verification artifacts (PDF)
- **Automated** test compilation, execution and result analysis (allows nightly runs)
- QA support by means **of review sheet preparation** and review status maintenance
- Synopsis **test case generator**
- Allows fine control on the granularity of the tests executed (full, partial, individual tests)
- Supports **single-core** or **multicore** configurations
  - SMP for PikeOS
  - AMP for PikeOS for MPU)

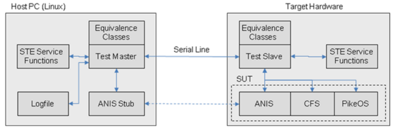


Figure 1Example of a PikeOS Test Environment for POSIX tesing purposes

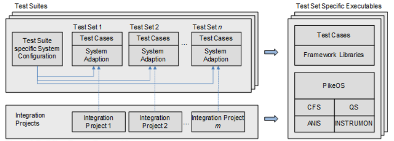


Figure 2 Building Target Executables

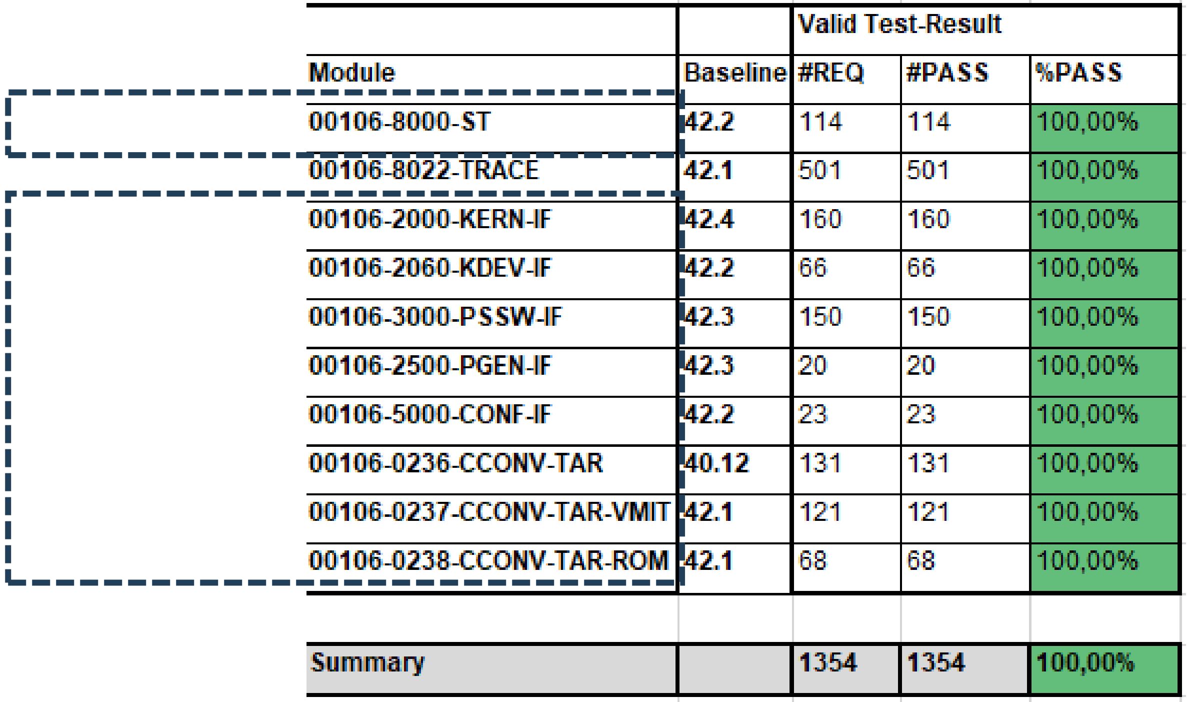
VALIDATION AND VERIFICATION INFRASTRUCTURE

SYSGO Test Framework (TFW)

- Extensible and **adaptable interface** for project specific setups (e.g. interface to target controller equipment for real HW)
- **Bi-directional interface** to the requirement management tool DOORS to exchange data between test suites and DOORS requirement documents
- **Interface** to the config management tool GIT to perform automated inspection of files
- **Generic interface to structural code coverage tools,** implementations for CodeTEST and Rapita Verification Suite (RVS) are available

SECURITY VALIDATION AND VERIFICATION RESULTS

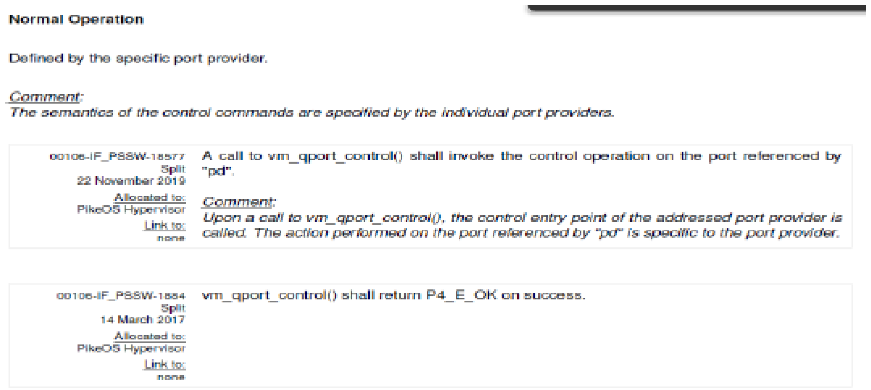
- In order to test and validate the security requirements (00106-8000-ST) a mapping to the existing requirements of the RTOS components has been established in a traceability matrix (TRACE).
- This TRACE document has been combined with the test results (TR) to summarize in one single document the security tracing and achievement during testing.



		Valid Test-Result		
Module	Baseline	#REQ	#PASS	%PASS
00106-8000-ST	42.2	114	114	100,00%
00106-8022-TRACE	42.1	501	501	100,00%
00106-2000-KERN-IF	42.4	160	160	100,00%
00106-2060-KDEV-IF	42.2	66	66	100,00%
00106-3000-PSSW-IF	42.3	150	150	100,00%
00106-2500-PGEN-IF	42.3	20	20	100,00%
00106-5000-CONF-IF	42.2	23	23	100,00%
00106-0236-CCONV-TAR	40.12	131	131	100,00%
00106-0237-CCONV-TAR-VMIT	42.1	121	121	100,00%
00106-0238-CCONV-TAR-ROM	42.1	68	68	100,00%
Summary		1354	1354	100,00%

SAMPLES

Requirements Document: 00106-3000-PSSW-IF.pdf



Normal Operation

Defined by the specific port provider.

Comment:
The semantics of the control commands are specified by the individual port providers.

00106-IF_PSSW-18577 Split 22 November 2019 Allocated to: PikeOS Hypervisor Link to: none	A call to vm_qport_control() shall invoke the control operation on the port referenced by "pd". *Comment:* *Upon a call to vm_qport_control(), the control entry point of the addressed port provider is called. The action performed on the port referenced by "pd" is specific to the port provider.*
00106-IF_PSSW-1884 Split 14 March 2017 Allocated to: PikeOS Hypervisor Link to: none	vm_qport_control() shall return P4_E_OK on success.

Test Case from 00106-3003-PSSW-TC.pdf

3.33.2 tc_03 Normal operation test of vm_qport_control().

GP_OK: method: TEST
Check that vm_qport_control() returns P4_E_OK when called with valid port descriptor and when the invoked kdev Gate Provider's control entry point returns P4_E_OK.

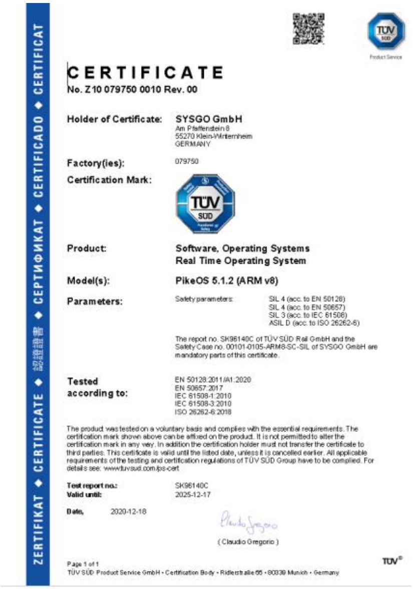
GP_CTRL: method: TEST
Check that vm_qport_control() has been entered by a test specific ioctl command. Test if the ioctl command's data is filled by the provider with an identifier.

Test LOG

```
[00106/ts_pssw_mpu] / vvbuild_results / tp.CommunicationPorts.portControl.res
1 run target
2 ##START##
3 date      |07.02.2023 10:49:15 UTC
4 identify  |test set name:
5 identify  |  tp.CommunicationPorts.portControl
6 identify  |test cases:
7 identify  |  TC 'tc_03' num_subtc=1   manual=0
8 identify  |  TC 'tc_04' num_subtc=1   manual=0
9 identify  |build by:
10 identify  |  pikeos@vvbuild7
11 identify  |build id:
12 identify  |  413e3296-36c6-3800-94c4-c212843647ff
13 identify  |target controller host name:
14 identify  |  vvbuild7
15 identify  |target controller machine id:
16 identify  |  c114657f-9632-8fe1-54c5-201ecde26ab6
17 identify  |target inventory number:
18 identify  |  none
19 identify  |channels:
20 identify  |  protocol    tcp link to 127.0.0.1:5000
21 tc.start  |tp.CommunicationPorts.portControl-tc_03
22 equ.start |tp.CommunicationPorts.portControl-tc_03|1
23 obj.subres|tp.CommunicationPorts.portControl-tc_03|1|GP_OK|S_PASS
24 obj.subres|tp.CommunicationPorts.portControl-tc_03|1|GP_CTRL|S_PASS
25 equ.end   |tp.CommunicationPorts.portControl-tc_03|1
26 obj.result|tp.CommunicationPorts.portControl-tc_03|GP_CTRL|O_PASS
27 obj.result|tp.CommunicationPorts.portControl-tc_03|GP_OK|O_PASS
28 tc.end    |tp.CommunicationPorts.portControl-tc_03
29 tc.start  |tp.CommunicationPorts.portControl-tc_04
30 equ.start |tp.CommunicationPorts.portControl-tc_04|1
31 obj.subres|tp.CommunicationPorts.portControl-tc_04|1|GP_OK|S_PASS
32 obj.subres|tp.CommunicationPorts.portControl-tc_04|1|GP_CTRL|S_PASS
33 equ.end   |tp.CommunicationPorts.portControl-tc_04|1
34 obj.result|tp.CommunicationPorts.portControl-tc_04|GP_CTRL|O_PASS
35 obj.result|tp.CommunicationPorts.portControl-tc_04|GP_OK|O_PASS
36 tc.end    |tp.CommunicationPorts.portControl-tc_04
37 summary   |4 O_PASS, 0 O_UNSUPPORTED, 0 O_UNTESTED
38 summary   |0 O_FAIL, 0 O_ERROR, 0 without result
39 date      |07.02.2023 10:49:16 UTC
40 ##END##
41 TEST RUN RETURN VALUE: 0
```

CERTIFICATION WITH TFW

- **Automatic Traceability (Requirements, Implementation, Test)**
  - Complete Automation (DOORS, GIT, VVBUILD, TFW)
  - Easy check of compliance and completeness
  - Early cross-checking and error correction
- **Cross-Standards Certification Model**
  - **for**
    - DO-178 (Avionic),
    - ECSS 40/80 (Space),
    - EN50128, EN50657 (Railway),
    - IEC61508 (Automation),
    - ISO26262 (Automotive)
  - Generic “Tailoring” Concept used, only one set of “corporate” plans and standards
  - All development life cycle documents are the same for every standard
  - Only plans and certification artefacts (e.g. Safety Case v. SW Accomplishment Summary) are generated according to the need of the specific industry.
- **“Proven-in-use” handling of Certification-Readiness**
  - For lower and highest safety levels (up to DO-178C DAL-A, ECSS Category A)
  - “Security certification” is handled with the same process model now extended with the dimension “Security”.
  - Well-known “notified bodies” for product and project certifications
  - Well-known “authorities” and expertise to handle “certifications”



ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Product Service

CERTIFICATE
No. Z10 079750 0010 Rev. 00

Holder of Certificate: **SYSGO GmbH**
Am Pfaffenstein 8
55270 Klein-Winternheim
GERMANY

Factory(ies): 079750

Certification Mark:

Product: **Software, Operating Systems**
Real Time Operating System

Model(s): **PikeOS 5.1.2 (ARM v8)**

Parameters: Safety parameters: SIL 4 (acc. to EN 50128)
SIL 4 (acc. to EN 50657)
SIL 3 (acc. to IEC 61508)
ASIL D (acc. to ISO 26262-6)

The report no. SK96140C of TÜV SÜD Rail GmbH and the Safety Case no. 00101-0105-ARM8-SC-SIL of SYSGO GmbH are mandatory parts of this certificate.

Tested according to: EN 50128:2011/A1:2020
EN 50657:2017
IEC 61508-1:2010
IEC 61508-3:2010
ISO 26262-6:2018

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. This certificate is valid until the listed date, unless it is cancelled earlier. All applicable requirements of the testing and certification regulations of TÜV SÜD Group have to be complied. For details see: www.tuvsud.com/ps-cert

Test report no.: SK96140C
Valid until: 2025-12-17

Date, 2020-12-18

Claudio Gregorio
(Claudio Gregorio)

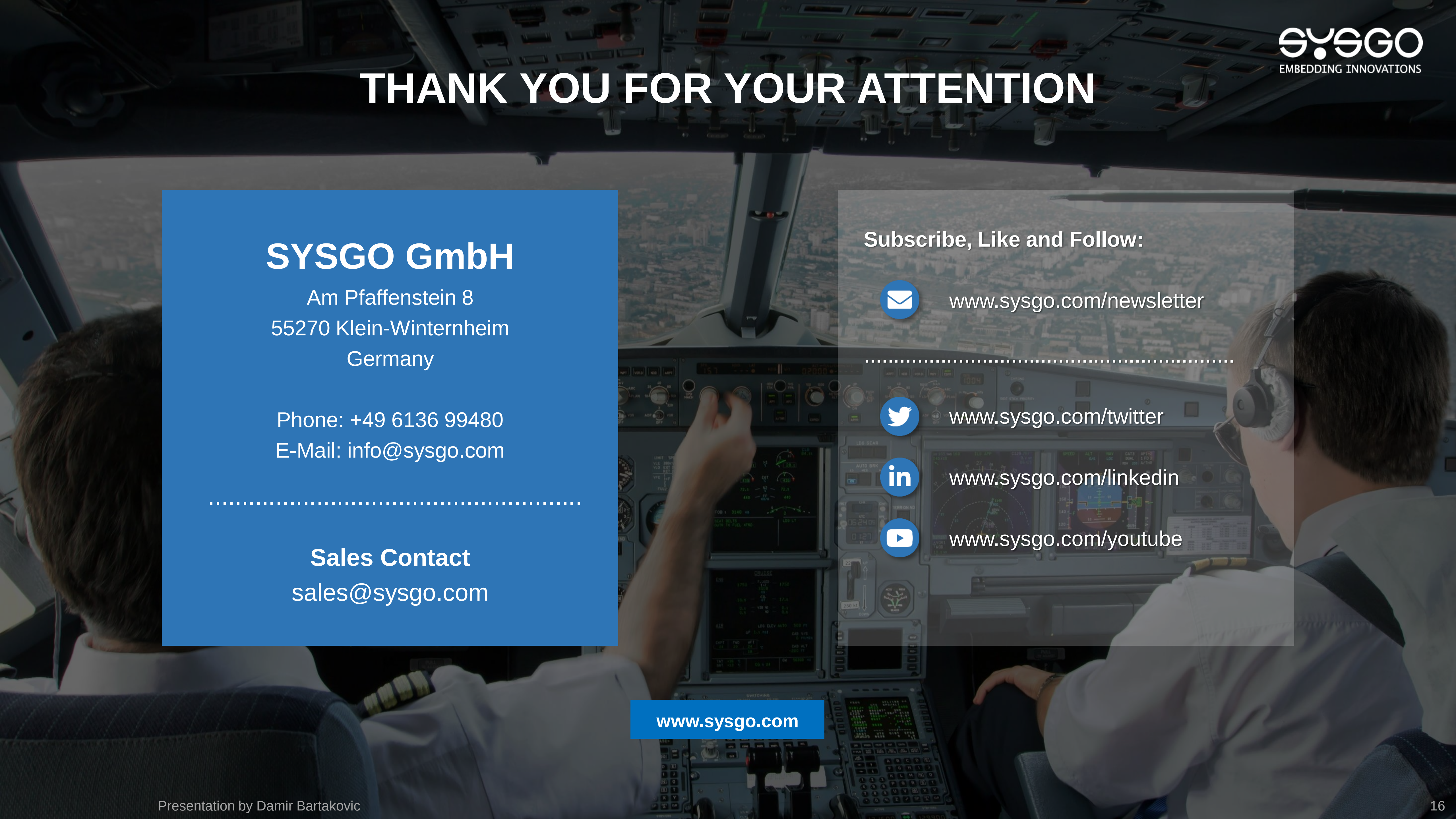
Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

CERTIFICATION STATISTICS (PIKEOS RTOS)

- **Detailed Specification of Functionality, Architecture and Design**
  - # of High Level Requirements: 1122
  - # of Low Level Requirements: 9225
  - **Ø 2.4 Source Code Lines (only cert parts) / Requirement**
  - # of document, source code and test case reviews executed: 728
- **Detailed Tests to cover Functionality and Structural coverage**
  - All tests are executed on all reference hardware (e.g. different architectures like ARM8, PPC, X86)
  - Approach to test on specific customer hardware (PikeOS PSP Validation)
  - # of test procedures: 2689
  - # test objectives: 18413
  - # of Test Source Code Lines: 1.6 M
  - # of decision point to be covered by testing: 4350
  - # of MCDC points to be covered by testing: 4313
  - **Ø 154 Test Source Lines / Requirement**
- **High Automation during Testing**
  - Usage of SYSGO test framework to
    - highly automate tests (100%) with nightly test runs and automatic target control
    - handling of target HW testing
    - Module, Inspection and Functional testing fully automated
    - All documents (test cases, test reports, structural coverage) will be generated as PDFs (Camera-ready verification artifacts)
    - All test tools are qualified up to the highest safety and security levels

CONCLUSION

- Security for space has become important in most recent times
- A RTOS with a prequalified set of documentation for security is the basis to provide all security "features" to be used for security for the SBRTOS.
- Security certification on system level need further investigation depending on the requirements for the SBRTOS.
- This V&V approach and packaging allows for the full V&V testing to be done on site on actual deployed HW, or early in the development process in a simulated environment before the HW is available



SYSGO
EMBEDDING INNOVATIONS

THANK YOU FOR YOUR ATTENTION

SYSGO GmbH

Am Pfaffenstein 8
55270 Klein-Winternheim
Germany

Phone: +49 6136 99480
E-Mail: info@sysgo.com

Sales Contact
sales@sysgo.com

Subscribe, Like and Follow:

www.sysgo.com/newsletter

www.sysgo.com/twitter

www.sysgo.com/linkedin

www.sysgo.com/youtube

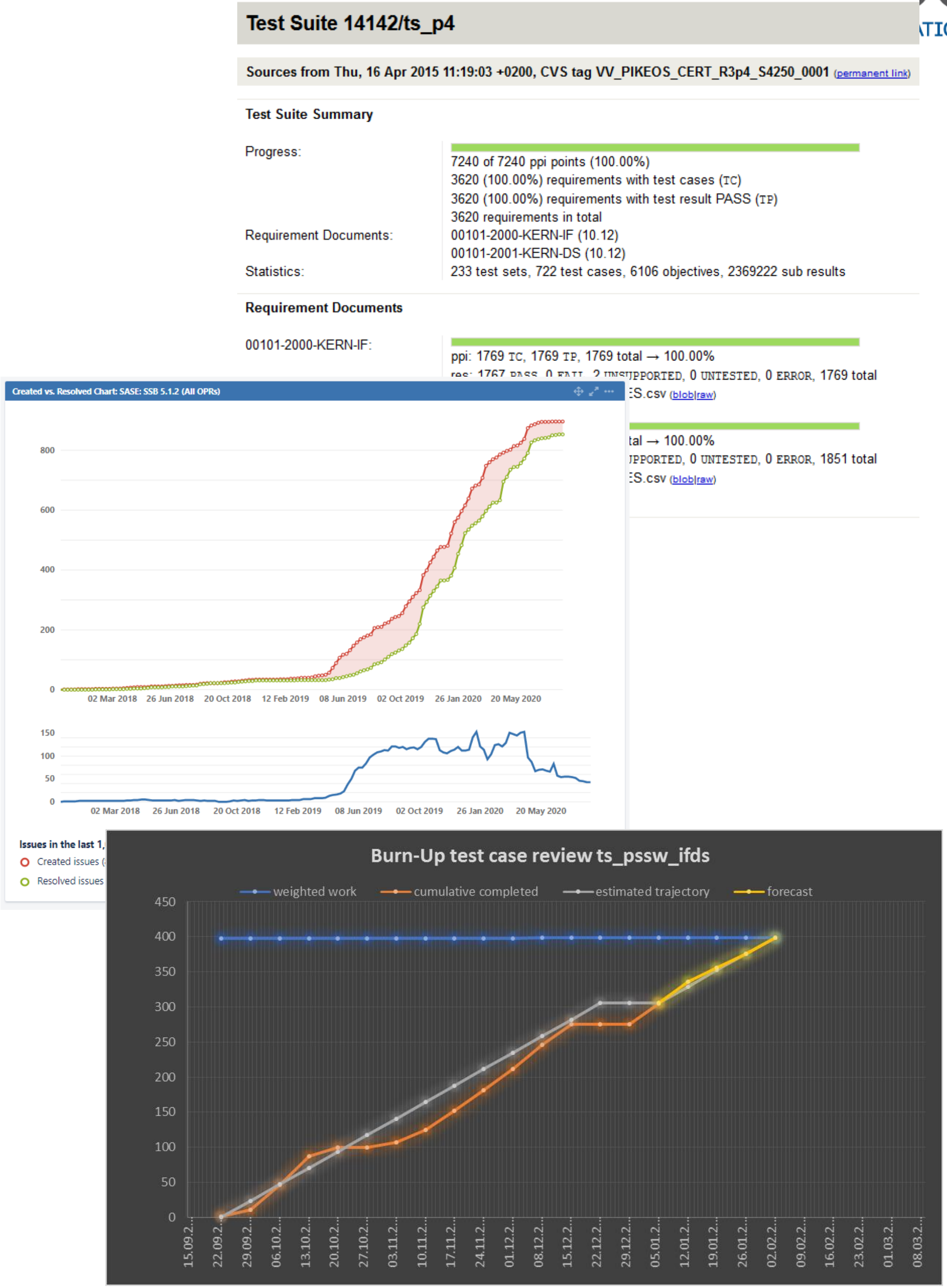
www.sysgo.com

PERFORMANCE EVALUATION

- **vvbuild** generates performance indicators based on tested requirement, result and review status

- **OPR classification** to analyze the impact of safety and security-relevant deviations

- **KPI:** Evaluation of Progress, Efficiency & Velocity



Test Suite 14142/ts_p4

Sources from Thu, 16 Apr 2015 11:19:03 +0200, CVS tag VV_PIKEOS_CERT_R3p4_S4250_0001 (permanent link)

Test Suite Summary

Progress:	7240 of 7240 ppi points (100.00%) 3620 (100.00%) requirements with test cases (TC) 3620 (100.00%) requirements with test result PASS (TP) 3620 requirements in total
Requirement Documents:	00101-2000-KERN-IF (10.12) 00101-2001-KERN-DS (10.12)
Statistics:	233 test sets, 722 test cases, 6106 objectives, 2369222 sub results

Requirement Documents

00101-2000-KERN-IF:	ppi: 1769 TC, 1769 TP, 1769 total → 100.00% res: 1767 PASS, 0 FAIL, 2 UNSUPPORTED, 0 UNTESTED, 0 ERROR, 1769 total ES.csv (blob|raw)
	tal → 100.00% JPPORTED, 0 UNTESTED, 0 ERROR, 1851 total ES.csv (blob|raw)