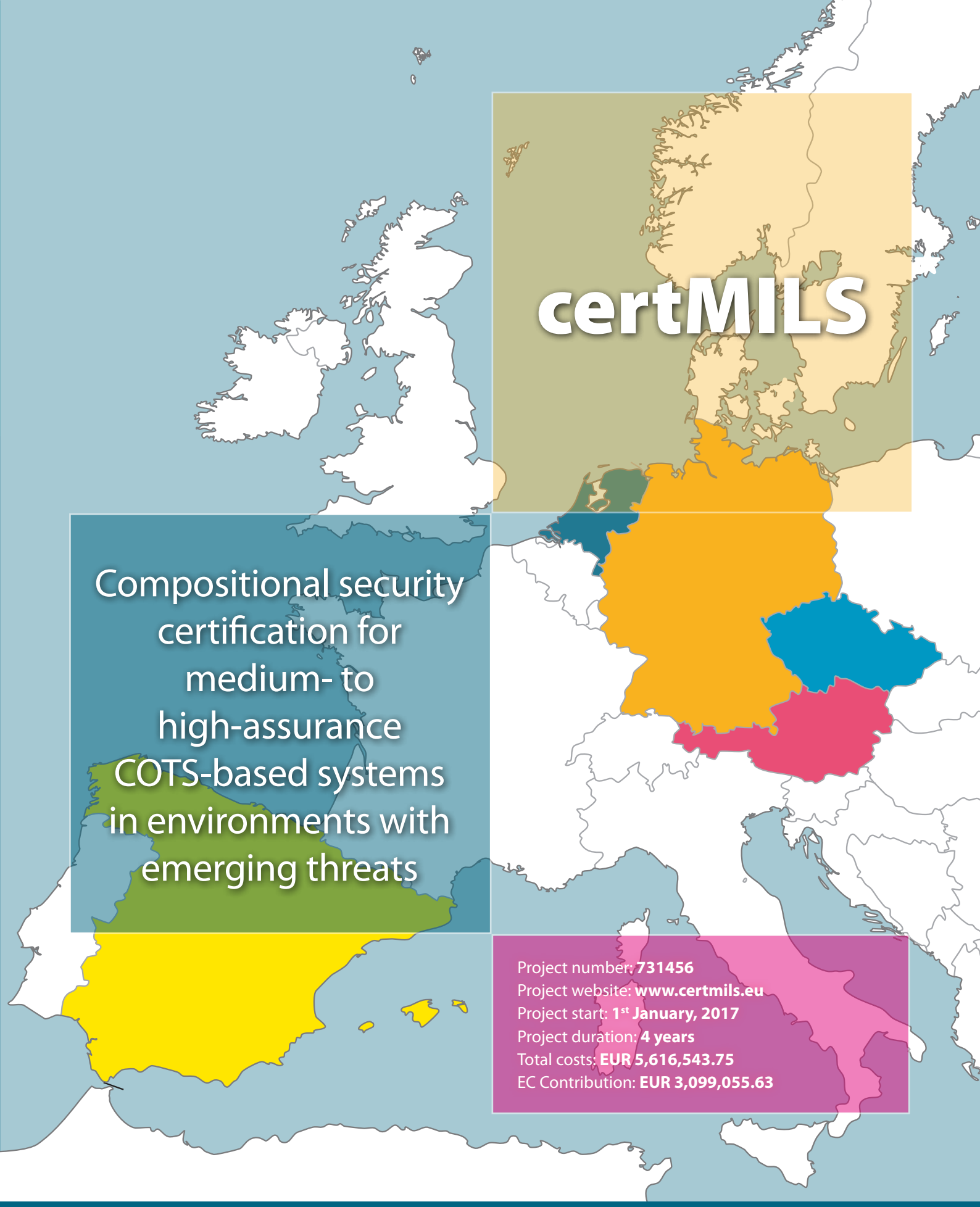


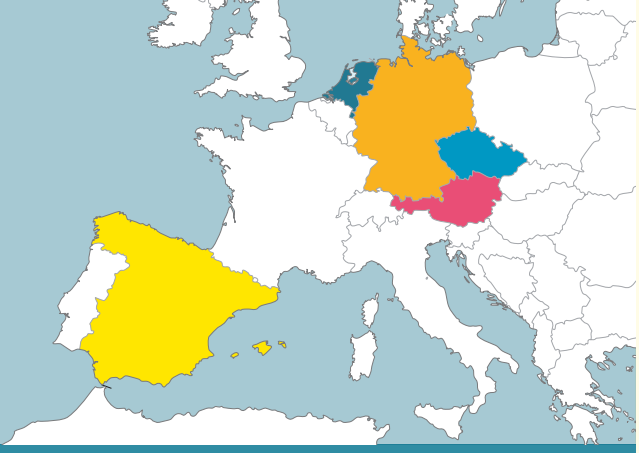
certMILS

Compositional security certification for medium- to high-assurance COTS-based systems in environments with emerging threats

Project number: **731456**
Project website: **www.certmils.eu**
Project start: **1st January, 2017**
Project duration: **4 years**
Total costs: **EUR 5,616,543.75**
EC Contribution: **EUR 3,099,055.63**

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

certMILS



certMILS Mission:

certMILS develops a security certification methodology for Cyber-physical systems (CPS). CPS are characterised by safety-critical nature, complexity, connectivity and open technology. certMILS aims to increase the economic efficiency and European competitiveness of CPS development, while demonstrating the effectiveness of safety & security certification of composable systems.

certMILS Motivation:

Previously isolated embedded systems have become connected to the Internet, thus becoming cyber-physical systems. For instance in transportation, for passenger as well as operator comfort, almost all means of transportation (airplanes, trains, cars, and ships) are networked. Due to the havoc potential of a malicious attacker, the security of cyber-physical systems has obtained a lot of interest. However, unlike many other IT systems, cyber-physical systems usually have already been heavily scrutinised for safety for decades. While the safety protection against accidental faults does not address security, there are already established safety methods as well as "safety certification stakeholders". Securing and certifying cyber-physical systems therefore must respect the existing safety certification processes. certMILS generates rich interaction between developers, evaluation laboratories and certification authorities in three European countries resulting in:

- Validated modular Protection Profile
- Standardised and validated methodology for evaluating and certifying high assurance products
- Guidelines for compositional security for developers and evaluators.

Concept:

certMILS aims to reduce the complexity of the certification of cyber-physical systems dramatically by use of a trustworthy MILS platform (Multiple Independent Levels of Security) within the cyber-physical system, which is simple, small, and certified for the highest level. Such a platform enables compositional security certification, which is applied in three different pilots. To be marketable as product for a large scope of ICT/cyberphysical systems, the platform has a powerful API configuration, supports open common and domain specific APIs (e.g. POSIX, ARINC) as well as consistently addresses existing domain safety standards/regulations.

Objectives:

A common downside to Cyber-physical systems (CPS) complexity and openness is a large attack surface and a high degree of dynamism that may lead to complex failures and irreparable physical damage. The legitimate fear of security or functional safety vulnerabilities in CPS results in arduous testing and certification processes. Once fielded, many CPS suffer from the motto: never change a running system. certMILS increases the economic efficiency and European competitiveness of CPS development, while demonstrating the effectiveness of safety & security certification of composable systems.

Objective 1: Transfer know-how in compositional safety certification to security certification

The first objective applies a compositional design and an accompanying compositional safety certification experience to a compositional security certification. Compositionality means increasing re-usage of COTS (Commercial Off-The Shelf) products and certified systems, based on a well-defined delegation of responsibilities between component developers and system integrators.

Objective 2: Make certification of composed systems affordable

certMILS makes certification economically flexible by combining certification and a more light-weight checking procedure ("compliance") for components of a lower criticality. This enables using feature-rich COTS components while keeping the certified system security.

Objective 3: Preservation of certified assurance throughout operational deployment

Objective 3 ensures secure update of composed systems in the field with certification/assurance maintenance to cover emerging threats and provide templates and guidance for flaw remediation.

Objective 4: Involvement of all stakeholders in different industry domains

certMILS will involve assurance cases from different representative industry domains in cyber-physical systems. The consortium and its advisory board representatively cover the roles of all relevant European stakeholders.

Objective 5: Certified European MILS platform and MILS Platform Protection Profile

certMILS aims to provide the first certified European MILS platform, which is a major building block and enabling technology for compositionally building secure cyber-physical systems.

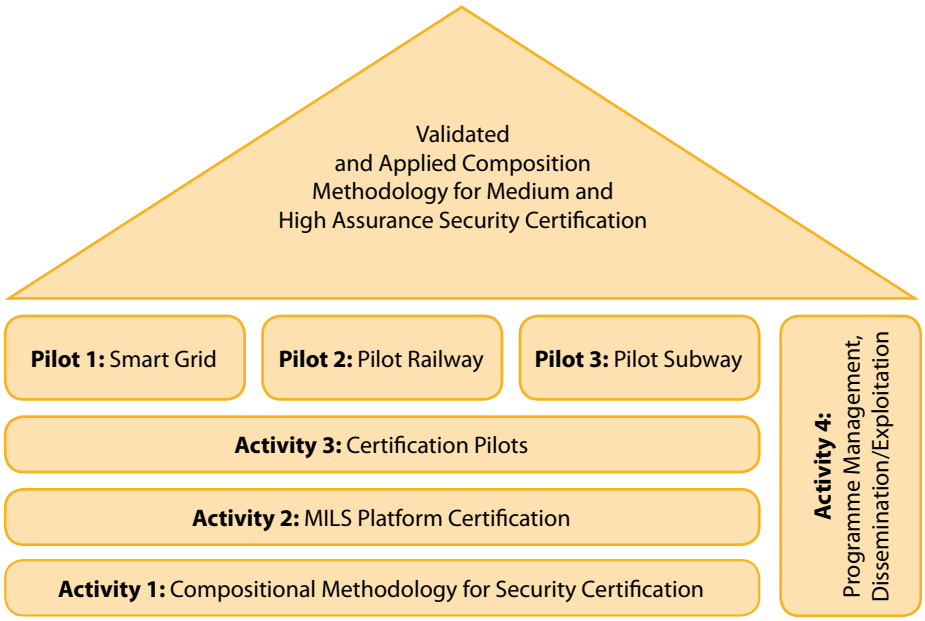
Objective 6: Develop and apply compositional certification methodology on three industrial pilots

Three industrial pilots apply the MILS approach to achieve security by design based on the MILS platform. Security evaluators use the certified MILS platform to do compositional certification according to certMILS methodology and industrial standards. Each pilot validates the results with the relevant authority.

Objective 7: Guidelines and templates for MILS certification

For our own use, but also as a means to interact with the community at large, certMILS will create and publish guidelines and templates for MILS certification for component developers, product integrators and evaluators. These will ease future certifications of MILS systems in particular, as well as of compositional systems in general.

certMILS structure and work packages:



Technical Approach:

certMILS has three technical activity lines and one management activity structured into ten work packages (WP) in order to increase efficient information exchange. They are processed within 48 months and every WP has its objectives and interfaces aligned with the certMILS concept and objectives.

Activity 1: Compositional Methodology for Security Certification
The first Activity consists of two WPs:

WP1: „Baseline for compositional evaluation“
The first WP defines the baseline for compositional security certification and the methodology and it identifies the list of existing supporting tools.

WP2: „Standardisation of MILS integration methodology“
WP2 develops the modular MILS Platform Protection Profile (PP) and supports the compositional security evaluation described in the PP.

Activity 2: MILS Platform Certification is split into three WPs:
Activity 2 is split into the following three WPs:

WP3: „MILS platform definition“
This WP defines the scope for the certification of the MILS platform and develops the CC Security target for the MILS platform.

WP4: „MILS platform enhancement“
WP4 prepares the implementation of the MILS platform for certification and develops the security testing approach. It develops security testing approach suitable for MILS platform and reusable for pilots.

WP5: „MILS platform certification“
This WP is responsible for the security evaluation and certification of the MILS platform.

Activity 3: Certification Pilots
The third Activity is divided into the three pilot WPs:

WP6: „Pilot Smart Grid“
WP7: „Pilot Railway“
WP8: „Pilot Subway“
These three specify pilots define its security architecture and security requirements. Activity 3 integrates the pilots from existing and COTS components on the MILS platform and it provides the evaluation and certification results for Activity 1.

Activity 4: Programme Management, Dissemination/Exploitation wraps the project by focusing on dissemination, communication, standardisation, exploitation and management activities.
There are two WPs:

WP9: “Communication, standardisation, dissemination and exploitation”
WP9 obtains inputs from all other WPs and ensures the communication/ dissemination of results to the outside parties and participating entities. WP9 supports the partners to exploit the achieved results and impacts the European and international market. Results within each other WP will lead to contributions to standardisation activities, coordinated by this WP.

WP10: “Project, risk, and innovation management”
The last WP draws from the input of all other WPs to ensure a successful project lifetime with respect to risk and innovation management. The management WP shows dependencies to all other WPs as it coordinates and ensures that the tasks are in line with the project work plan in order to reach the common goals of certMILS.

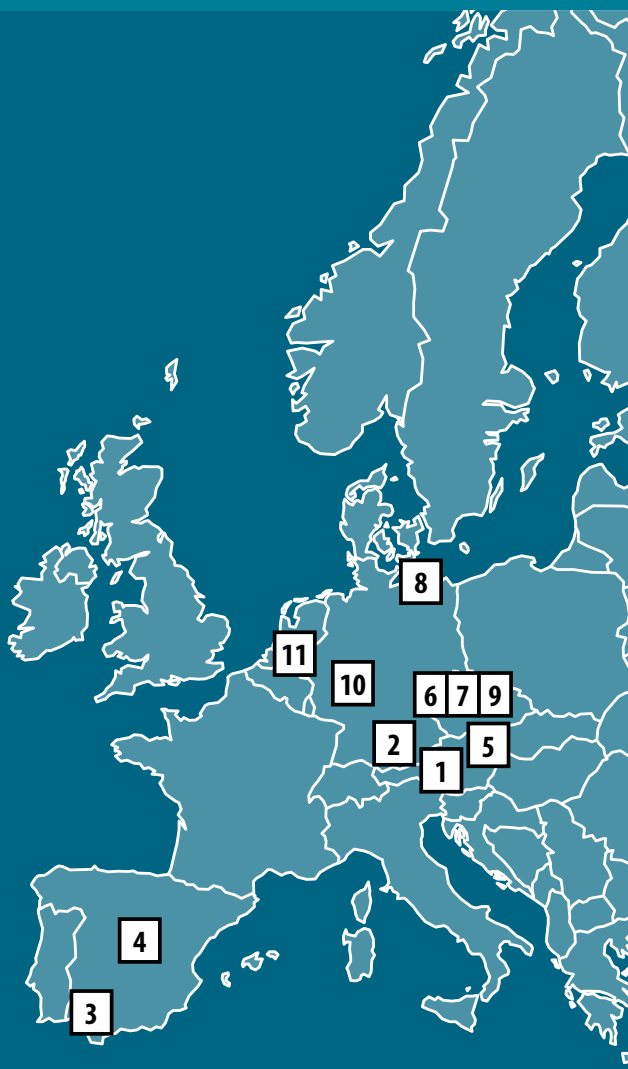
Contacts:

Project Coordinator:
Dr. Klaus-Michael Koch
Technikon Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a
9500 Villach, Austria
Tel.: +43 4242 233 55
Email: coordination@certmils.eu
Web: www.certmils.eu

Technical Leader:
Dr. Sergey Tverdyshev
SYSGO AG
Am Pfaffenstein 14
55270 Klein-Winternheim, Germany
Tel.: +49 6136 9948 788
Email: sergey.tverdyshev@sysgo.com

Consortium:

The certMILS consortium consists of 11 partners (including linked third parties) from 5 different EU countries. It is a thoroughly selected mix of partners who complement each other with their competencies, experience and ambition at high level.



Project Partners:

1 **Technikon Forschungs- und Planungsgesellschaft mbH, Austria [Villach]**

2 **ATSEC Information Security GmbH, Germany [Munich]**

3 **Schneider Electric España SA, Spain [Sevilla]**

4 **Epoche and Espri SL, Spain [Molar]**

5 **Thales Austria GmbH , Austria [Vienna]**

6 **Unicontrols A.S., Czech Republic [Prague]**

7 **SYSGO s.r.o, Czech Republic [Prague]**

8 **University of Rostock, Germany [Rostock]**

9 **Elektrotechnicky zkusebni ustav, s.p., Czech Republic [Prague]**

10 **SYSGO AG, Germany [Klein-Winternheim]**

11 **NXP Semiconductors N.V., Netherlands [Eindhoven]**