Newsletter

May 2017 - Issue 1

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

Main Project Information

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.

The constant security-related news and security bulletins make evident how insecure currently deployed ICT systems are. To tackle this challenge we need to provide an assurance within the system and its components, i.e. instead of "blind" trust we need evidence-based trustworthiness. Traditional certification schemes conservatively require assessment of the entire integrated system for certification. Due to system complexity, number of functions, and usage of Commercial Off-The Shelf (COTS) components, this approach became infeasible.

In this Issue

Message from the Coordinator

The intention of this Newsletter is to open a new communication channel in order to provide news on the project progress and to discuss ongoing topics relevant to **certMILS** for internal and external project partners, stakeholders and all other interested bodies. For more detailed information about and around the project we warmly invite you to have a look on our project website, which is constantly kept up-to-date with the latest project related news: www.certmils.eu.

The project has successfully started with the Kick-Off meeting in January 2017 and since then it has been in its initial stages of formation. certMILS will achieve major impact because technology-wise the consortium operates at a high TRL level close to security market, uses proven security-by-design (MILS) technology, and uses system design approach which is tightly coupled with security evaluation and security certification. This allows certMILS to develop technology prototypes early enough for later security evaluation and certification.

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.

Upcoming Events

- PikeOS Workshop, 28th - 30th June 2017, Mainz/Germany
- certMILS Technical Meeting, 3rd - 4th July 2017, Vienna/Austria

MILS Community

The MILS Community is a global international, open membership, not-for-profit technology consortium that will become the leading competence network on MILS architecture and technologies.

Key Data:

Start Date:	1st of January 2017
End Date:	31st of December 2020
Duration:	48 months
Project Reference:	731456
Project Budget:	€ 5,616,543.75
Project Funding:	€ 3,099,056.63

Consortium:	11 partners (5 countries)
Project Coordinator:	Dr. Klaus-Michael Koch coordination@certmils.eu
Technical Leader:	Dr. Sergey Tverdyshev sergey.tverdyshev@sysgo.com
Project Website:	www.certmils.eu

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

FOLLOW US ON twitter

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

Newsletter

May 2017 - Issue 1

Technical Approach

The certMILS project has three technical activity lines and one management activity structured into ten work packages in order to increase efficient information exchange. The first activity **"Compositional Methodology for Security Certification"** consists of two WPs: **WP1 "Baseline for compositional evaluation"** which 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"** 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 the following three WPs: **WP3 "MILS platform definition"** , that defines the scope for the certification of the MILS platform and develops the CC Security target for the MILS platform. **WP4 "MILS platform enhancement"** prepares the implementation of the MILS platform for certification and develops the security testing approach, suitable for MILS platform and reusable for pilots. **WP5 "MILS platform certification"** is responsible for the security evaluation and certification of the MILS platform. **T**he third activity **"Certification Pilots"** is divided into the three pilot WPs: **WP6 "Pilot: Smart Grid", WP7 "Pilot Railway"** and **WP8 "Pilot Subway".** These three pilots define the security architecture and security requirements. Activity 4: **"Programme Management, Dissemination/Exploitation"** consists of two WPs. **WP9 "Communication, standardisation, dissemination, and exploitation"** supports the partners to exploit the achieved results and impacts on the European and international market. Results within other WPs will lead to contributions to standardisation activities, coordinated by this WP. **WP10 "Project, risk, and innovation management"** receives 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 has a coordination function and ensures that the tasks are in line with the project work plan in order to reach the common goals of certMILS.

certMILS public deliverables submitted [M01-M03]:

- **D9.1** Internal and external IT communication infrastructure and project website
- **D10.1** Project Quality Plan

certMILS upcoming public deliverables [M04-M06]:

- **D1.1 Regulative baseline**

Publications

- **"Security by Design: Introduction to MILS"; Embedded World Conference 2017; S. Tverdyshev**
- **"Ease Standard Compliance by Technical Means via MILS"; Embedded World Conference 2017; S. Nordhoff, H. Blasum**

Ongoing Activities

After the successful project kick-off each partner has enthusiastically looked into their tasks within the particular WPs and started progress towards the objectives. The first deliverables have been submitted and quite some work has been performed during the first four project months. Currently the consortium is working on the functionality definition, such as a security target, candidates for modular extensions, and the state of the art of compositionality evaluation. Furthermore, discussions on security testing are going on. Additionally, the table of content for D6.1 "Compositional design of the smart grid pilot", D7.1 "Compositional design of the railway pilot" and D8.1 "Compositional design of the subway pilot" have been created. Apart from that, the HW/SW platform as a subject of certification has been specified and made ready for internal discussion. Moreover, the project website and information platform have been set up. A project logo, leaflet, announcement letter and press releases have been created and published. Furthermore, a Twitter and LinkedIn account has been established. D9.1 "Internal and external IT communication infrastructure and project website" has been submitted to the EC.

Key Data:

Start Date:	1st of January 2017
End Date:	31st of December 2020
Duration:	48 months
Project Reference:	731456
Project Budget:	€ 5,616,543.75
Project Funding:	€ 3,099,055.63

Consortium:	11 partners (5 countries)
Project Coordinator:	Dr. Klaus-Michael Koch coordination@certmils.eu
Technical Leader:	Dr. Sergey Tverdyshev sergey.tverdyshev@sysgo.com
Project Website:	www.certmils.eu

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

FOLLOW US ON twitter