Newsletter

February 2018 - Issue 2

cert MILS

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

Message from the Coordinator

Since the last newsletter in May 2017, the consortium is working on the first draft of the **Base MILS Platform Protection profile (PP)**, which is a Common Criteria object. The scope of the PP is to serve a basis for a **certified European MILS platform.**

In addition, the **certMILS** team is currently planning the **4th International Workshop on MILS: Architecture and Assurance for Security Systems,** which will be co-located with the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2018) in Luxembourg.

In this Issue

- **Message from the coordinator**
- **Technical/GA/AB Meeting, Olbramovice**
- **Upcoming events: 4th International MILS workshop @DSN2018**
- **Project Progress / Highlights**
- **MILS Community**

certMILS Technical/GA/AB Meeting in Olbramovice/Czech

In January 2018, the **certMILS Technical and General Assembly Meeting** as well as the first **Advisory Board Meeting** took place in Olbramovice/ Czech Republic.

The **certMILS** team discussed the current project status and the planning of upcoming tasks and reports. Five external experts from five different companies joined the first Advisory Board meeting in order to assist the **certMILS** consortium by providing advice for the work within the project.

Upcoming Events

- **3rd Annual Rail Cyber Security Summit**
  14th March 2018, London/UK
  https://www.railcybersecurity.com/

- **1st UIC Global Conference on Signalling—The Evolution of ERTMS**
  26th—28th March 2018, Milan/Italy
  https://www.uic.org/com/uic-e-news/567/article/1st-uic-global-conference-on-signalling?page=thickbox_enews

- **Common Criteria Users Forum Meeting**
  24th—26th April 2018, Trondheim/Norway
  http://www.ccusersforum.org

- **4th International Workshop on MILS: Architecture and Assurance for Secure Systems co-located with DSN 2018**
  25th June 2018, Luxembourg
  http://mils-workshop-2018.mils.community

MILS Community

If you want to

- **learn more** on the MILS Community,
- **participate** to the early phases of the Community creation,
- **be informed** about the status of the Community,

then **send us an e-mail** to community@mils.community OR **subscribe to the MILS mailing list** mils@lists.technikon.com.

The MILS mailing list is a public mailing list for discussions of Multiple Independent Levels of Security (MILS) architectural approach for security and safety, MILS components, MILS implementations, MILS research, MILS use-cases, real-time separation kernels, MILS evaluation and certification, MILS testing and vulnerability, and analysis of MILS systems.

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:	€ 3,999,055.63

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

Linked in

🐦 **@certMILS_h2020**

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

Newsletter
February 2018 - Issue 2

Project Progress / Highlights

Currently, we are in month 14 (February 2018) of the certMILS project. Within the first project year the work progress was well on track.
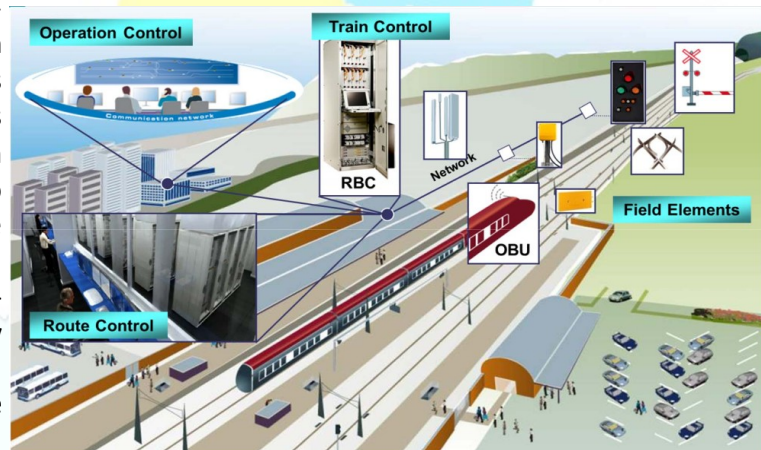
A report on the state-of-the-art for compositional evaluations has been written. This report describes the different ways compositions are currently performed for evaluations using ISO/IEC 15408 (Common Criteria) as of today.

The certMILS team is currently working on a Common Criteria object, which can be used as an stand-alone Protection Profile or as a Base-PP for a modular PP (Base-PP plus extended packages). The scope of this Base-PP is a Separation Kernel that can serve as a basis for a **MILS platform**. The Separation Kernel provides a basis for multiple partitions where each partition gets its resources assigned by the Separation Kernel. The minimum set of resources that the Separation Kernel must be able to assign to partitions are computer memory and processing time. As such, the Separation Kernel is an operating system with minimized functionality leaving higher level functions, usually provided by a general purpose operating system like file systems, network protocols and application management, to be provided by the partitions. The Base-PP contains the basic functions of the Separation Kernel and it will be accompanied by a number of extensions / PP-modules addressing areas where specific Separation Kernels handle functions in a different way. Current candidates for PP-modules are

- Input/ Output Memory Management Unit (IOMMU)
- Platform Support Package (PSP)
- Security Audit
- Real-time capabilities
- Integrity of data stored
- Crypto
- Secure boot
- Secure Update
- Partitioned Network components
- Information flow
- Management module-Dynamic partition manage-

We are seeking external feedback on the PP and its modules, please contact us if you are interested.

Moreover, the team is working on the Smart Grid pilot definition. In addition to that, Common Criteria, IEC 62443 and its applicability to the Smart Grid pilot have been analysed. The IEC 62443 series of standards generally specify requirements for security capabilities. These capabilities may be technical capabilities (security mechanisms) or process capabilities (human procedures) for a MILS system. Therefore, the certMILS team is also an active member in several Work Groups and Task Forces under the IECEE and other organisations. Furthermore, a scenario for evaluation definition has been established and the implementation of the medium assurance pilot has been done. The Smart Grid pilot is based on an IACS of an electrical substation, and implements remote terminal units (RTU) with industrial protocols and security functionality. An evaluation board for the high assurance has been acquired and the software installation has been started. Furthermore, a first presentation of the use case (RTU) took place. In addition to all these achievements the consortium gave presentations and talks at different conferences. For example Michael Paulitsch from Thales, Austria gave an invited talk at the "**2017 Safety meets Security Conference**" about "Safety and Security in Ground Transportation Systems" (see illustration).

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:	€ 3,999,055.63

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

@certMILS_h2020