Vessedia

VERIFICATION ENGINEERING OF SAFETY AND SECURITY CRITICAL INDUSTRIAL APPLICATIONS

MAIN PROJECT INFORMATION

VESSEDIA aims at enhancing and scaling up modern software analysis tools to use them on medium-criticality applications such as IoT. The technical goals of this Project are to improve the security and reliability of connected embedded software applications, to promote formal methods and make them more accessible, to build a flexible methodology for safety and security analysis, to test specific formal methods and to provide tool support for the security evaluation and certification processes.

To reach all this goals VESSEDIA develops measures enabling to quantify a V&V process, builds collaborative and smart user interfaces, provides High-level models for Verification and Validation (V&V), builds strong links with Common Criteria for the certification for medium criticality applications and will provide a new ISO standard.

Newsletter / September 2018 - Issue 3

Consortium
10 partners (7 countries)

Project Coordinator
Dr. Klaus-Michael KOCH
coordination@vessedia.eu

Technical Leader
Dr. Armand Puccetti
armand.puccetti@cea.fr

Project reference: **731453**
Project website: **www.vessedia.eu**

Project start: **1st January, 2017**
Duration: **3 years**

Total cost: **EUR 4,192,058.75**
EC contribution: **EUR 4,192,058.75**

PROJECT STATUS UPDATE

During the first project period (M01-M18), the project has achieved significant work that can be described in different research streams:

Three use-cases (Contiki OS, 6LoWPAN, experimental Aircraft Maintenance System) are running in parallel and performed the following tasks:	- Definition of the precise perimeter for analysis and of high level security and safety properties. - Set up of the project analysis tools and training. - First round of analyses (on-going).
Research and development to solve the technical problems in the analysis tools. This includes the following tasks that are under way:	- Improvements of the core tools Frama-C, VeriFast, Diversity, and FlowArmor. - Improvements of related plug-ins, such as E-ACSL and Frama-clang. - Improvements of Contiki-OS use-case, with a better global structure and more generic datastructures. - Connections between the formal analysis tool Frama-C and testing tool AFL and between Frama-C and modelling tool Diversity. - Design of new GUI and a client-server proof architecture for Frama-C. - Improvements to the ACSL++ specification language for C++.

Research on methodologies by integrating the end-users' concrete needs, the economic concerns and the quality measurements.

MEETING IN LEUVEN

From 10th to 11th July 2018 another VESSEDIA Advisory Board (AB) and Technical meeting took place at KU Leuven in Belgium. Within the framework of the Advisory Board Meeting on the first day, the technical leader of VESSEDIA presented a status up-date of the project. After this short update, some Work package (WP) leads presented the current status and the progress of their WPs followed by the presentation of the two use-cases "Contiki-OS" and "6LowPAN". Fruitful discussions took place which will be beneficial for the future project progress. The VESSEDIA team received valuable feedback and comments to different aspects, especially for the planed "Verified in Europe" label.

The second day was dedicated to the Technical Meeting where all WPs were presented by the leads. From an organizational point of view, also upcoming meetings and the VESSEDIA workshop in spring 2019 were discussed.

DELIVERABLES AND EVENTS

SUBMITTED PUBLIC DELIVERABLES

In June, month 18 of the Project, the following Deliverables have been submitted. Some of them were already published on the **VESSEDIA Website**. The documents have gone through the consortiums internal review process and are still subject to the review of the European Commission. Updates to the content may be made at a later stage.

- ***Modelling framework description*** deals with the modelling framework for the development of secure software. The goal of this framework is to close the gap between high-level textual requirements in an architecture model and low-level properties in the code.
- ***Basic analyzers intermediate release:*** Initial version of front-ends and specification libraries, improved analyzers and prototypes of new analyzers.
- ***Methodological report for modular reasoning for system validation and verification*** describes the combination between high-level system reasoning with Diversity and low-level code verification with Frama-C. To propose a solution bridging this gap for subsystems components that are implemented as software coded in C is the goal of this Deliverable.
- ***Metrics for VESSEDIA tools in quality assurance*** proposes and defines metrics, which can be helpful during the verification and evaluation process. For each metrics a implementation guidelines for Frama-C developers is specified, but the metrics ideas can also be used in other tools such as VeriFast.
- ***VESSEDIA approach for security evaluation*** describes a proposed security evaluation methodology for the VESSEDIA project. The methodology defined in this Deliverable is to be executed in later phases of the project and will be documented in following deliverables. It also collects and describes the state of-the-art of certification frameworks, and the VESSEDIA and STANCE tools developed by partners that will be used in the security evaluation in later phases.
- ***Inria's use case intermediate report*** presents the verification effort performed during the period M7-M18 of the project on the Contiki operating system. This verification is conducted using the Frama-C platform.
- ***CEA's use case intermediate report*** discusses the status of the analysis of the source code associated to a number of critical functionalities of the CEA use case, i.e. the 6LowPAN management platform.
- ***DA's use case intermediate report*** presents the results achieved at M18 for its experimental "Aircraft Maintenance System".

UPCOMING PUBLIC DELIVERABLES

- Preliminary version of the platforms
- Benchmark for evaluating VESSEDIA tools

DISSEMINATION ACTIVITIES

VESSEDIA partner plan to participate in the following events:

- **InnoTrans 2018**
  18th – 21st of September 2018
  @Berlin, Germany
- **IEEE Cybersecurity Development Conference (SecDev)**
  30th of September – 2nd of October 2018
  @Cambridge, MA, USA
- **Workshop of the CHARIOT project**
  11th of October
  @Rome, Italy

Follow **VESSEDIA** on:

This project has received funding from the European Union's Horizon 2020 Programme for research and innovation under grant agreement No 731453.