Newsletter

May - Issue 1

Vessedia

VESSEDIA
Verification Engineering of Safety and Security Critical Industrial Applications

Main Project Information

VESSEDIA proposes to **enhance and scale up modern software analysis tools to enable using them on a wider range of applications** than embedded safety-critical applications (in the nuclear, transportation, energy supply, process control and space areas). Developers will benefit rapidly from the outcome of the project when developing connected applications. At the forefront of connected applications is the Internet of Things (IoT), whose growth is exponential and whose security and safety risks are real (for instance in hacked smart phones or smart home devices). VESSEDIA will take this domain as a target for demonstrating the benefits of using our tools on connected applications.

The aim of this project consists in **making formal methods more accessible for application domains** that want to **improve the security and reliability of their software applications** by means of formal methods. In order to attain a solution to the challenges the **following objectives** were set:

- **Objective 1:** Drastically improving security verification tools
- **Objective 2:** Quantification of the verification process
- **Objective 3:** Building collaborative and smart user interfaces
- **Objective 4:** Formal Methods for non-highly-critical domains
- **Objective 5:** Management of verification data
- **Objective 6:** Higher-level models for verification
- **Objective 7:** Building strong links with existing certification practices

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 **VESSEDIA** 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.vessedia.eu. The project has successfully started with the kick-off meeting in January 2017 and since then the project has been in its initial stages of formation. Research on safety and security verification methodologies has been done and an initial draft of the security requirements for connected medium security-critical applications has been implemented. The next milestone will be in September 2017.
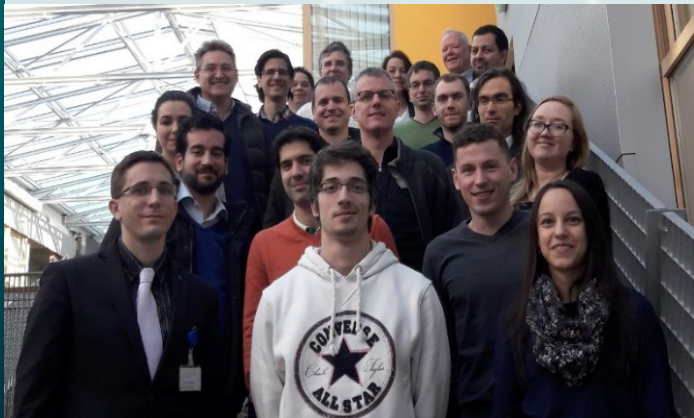
Kick-off Meeting

On 19th and 20th January 2017 the VESSEDIA consortium met at the Kick-Off-Meeting in Paris. The first day was dedicated to get to know each other ant to organize the further collaboration of the project partner. Afterwards the technical work packages were presented. Discussions and socializing continued during a common dinner in a less formal atmosphere. The second day focused on use cases and tools and ended with discussions on the next steps in the project.

Key Data:

Start Date:	1 st of January, 2017
End Date:	31 st of December, 2019
Duration:	36 months
Project Reference:	731453
Project Costs:	€ 4.192.058,75
Project Funding:	€ 4.192.058,75

Consortium:	10 partners (7 countries)
Project Coordinator:	Dr. Klaus-Michael Koch
	coordination@vessedia.eu
Technical Leader:	Dr. Armand Puccetti
	armand. puccetti@cea.fr
Project Website:	www.vessedia.eu

Linked in

FOLLOW US ON twitter

VESSEDIA

Verification Engineering of Safety and Security Critical Industrial Applications

Technical Approach

The VESSEDIA project will last **36 months** and will be organised in **7 work packages**. **WP1 "Safety and Security Verification Methodologies"** will develop the methodologies for using the toolbox developed in WP2. This includes the definition of specific aids and methods adequate for the use-cases of the project as well as GUI (Graphical User Interface) developments to support them. **WP2 "Integrated Verification Toolbox development"** is in charge of developing the tools for the V&V (Verification & Validation) of safety and security properties of C and C++ source code and can be seen as the core part of the project. This is also expressed by the highest number of effort foreseen in this WP. The different tools are integrated into a single toolbox that will be packaged and distributed by the project (in WP5). **WP3 "High-level models for software verification"** defines new models for representing the different items handled during a software development and verification activity. This includes design models, specifications and proofs models. **WP4 "Quality assurance and certification"** is in charge of developing metrics for the quantitative assessment of security V&V objectives and results for software development projects using the verification tools developed in WP2. It will also analyze VESSEDIA impacts on quality assurance, security evaluation and certification, from tooling and methodological standpoints. **WP5 "Use-cases"** demonstrates how the above tools and methodologies apply to industrial applications with well identified security and safety requirements. We will perform several medium-scale use-cases to measure quantitatively and qualitatively the efficiency and effectiveness of the tools, methodologies, and metrics. **WP6 "Dissemination, Communication, Exploitation, Standardisation and Training"** will develop 1) a standardisation plan that aims at building a new standard for the safety and security in critical software domains, 2) an exploitation plan to formalise the promotion of the tools, and 3) several communication, dissemination as well as training activities. **WP7 "Project, Risk, and Innovation Management"** is devoted to project risk and innovation management to ensure progress at the technical level as well as administrative management allowing proper steering of the project and interactions with the EC.

Submitted public deliverables:

- **D6.1** "Internal and external IT communication infrastructure and project website"
- **D7.1** "Project Quality Plan"

Scientific Publications:

- **ACSL By Example - Towards a Verified C Standard Library** *(J. Burghardt, R. Clausecker, J. Gerlach, H. Pohl for Frama-C Silicon in April 2017)*
- **Static Analysis and Runtime-Assertion Checking: Contribution to Security Counter-Measures** *(D. Pariente, J. Signoles for SSTIC in June 2017)*

Upcoming Conferences and Meetings:

- **VESSEDIA Technical Meeting**, 31th May - 1st June, Paris
- **Frama-C & SPARK Day** - Formal Analysis and Proof for Programs in C and Ada on 30th May 2017 in Paris, France
- **SSTIC 2017** - Symposium sur la sécurité des technologies de l'information et des communications on 7-9th June 2017 in Rennes, France

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 last 6 months. The work in WP1 has been swiftly started with respect to the concerned tasks 1.1, 1.2, 1.4, and 1.5. Conference calls and face-to-face meetings have been conducted to exchange on the progress of work and to discuss technical details. Most importantly, there exists already an early draft for D1.1. Further, a project website and information platform has been set up, a project logo, leaflet, an announcement letter and press releases have been created. Additionally, a Twitter and LinkedIn account were established.

Linked in

FOLLOW US ON twitter