VESSEDIA

Verification Engineering of Safety and Security Critical Industrial Applications

Project reference: **731453**
Project website: **www.vessedia.eu**
Project start: **1st January, 2017**
Duration: **3 years**
Total costs: **EUR 4,192,058.75**
EC contribution: **EUR 4,192,058.75**

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

Vessedia

Mission of VESSEDIA:

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.

Motivation:

In the fast evolving world we live in, the Internet has brought many benefits to individuals, organisations and industries. With the capabilities offered now (such as IPv6) to connect billions of devices and therefore humans together, the Internet brings new threats to the software developers and VESSEDIA will allow connected applications to be safe and secure. With software powering more than 80% of the functionalities inside modern-day ICT systems, the trustworthiness and security of these codes can be a major differentiator. From industrial process control and aircraft navigation system, to electricity supply grids and supervision networks, this observation has extended in the past few months to networked everyday objects such as health tracking devices or home automation appliances.

Concept:

VESSEDIA will tackle this challenge by

- developing a methodology that allows one to adopt and use source code analysis tools efficiently and produce similar benefits in other application domains of lower criticality than for highly-critical applications (i.e. an exhaustive analysis and extraction of faults)
- providing an enhance toolbox (Frama-C) to enable easy and efficient use by developers
- demonstrating the new toolbox capabilities on typical IoT applications including an IoT Operating System (Contiki)
- developing a standardisation plan for generalising the use of the toolbox to a wider set of applications
- contributing to the Common Criteria certification process
- defining Security Certification Levels (SCL) for lower critical IoT devices where Common Criteria certification is not convenient in practice
- defining a label "Verified in Europe" for validating software products with European technologies such as Frama-C.

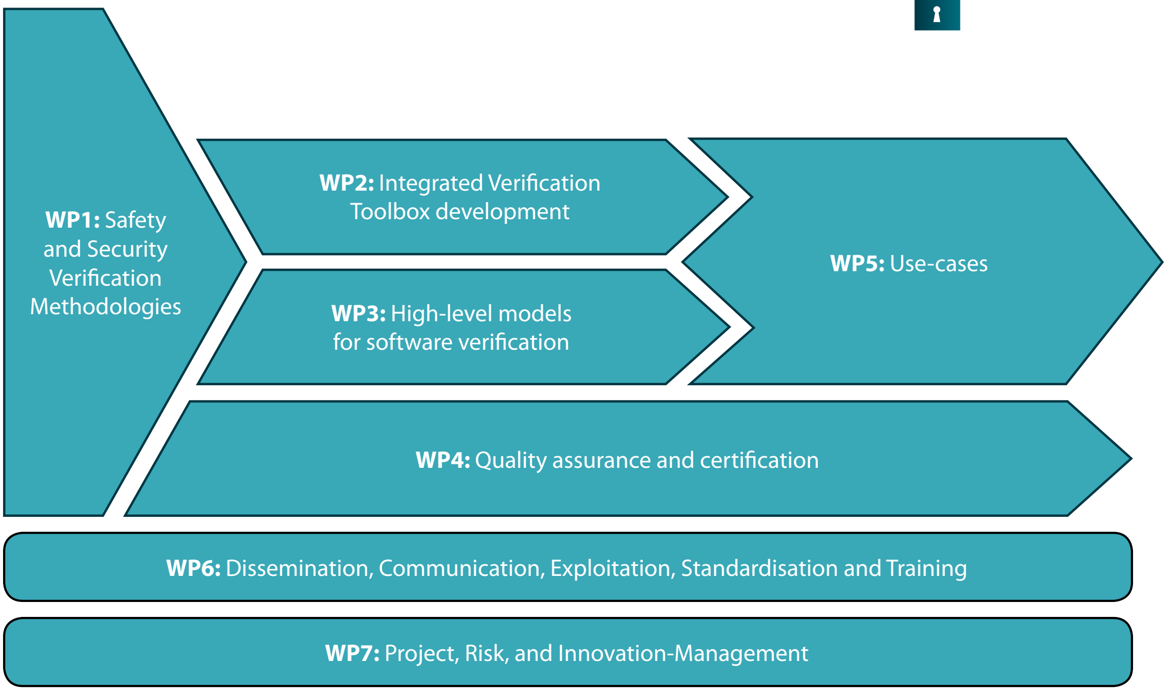
Objectives:

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

Objectives 1, 2, 3, 5 and 6 build and improve the tools that support developers in their daily analyses. We will improve existing tools and integrate them in development environment so that developers can model their application and write high quality source code. On top of these objectives is the development of a Methodology (Objective 4) to put Formal Methods to use in a real world scenario, with flexibility and cost-effectiveness. Helping to comply with a Common Criteria certification is the goal of Objective 7.

VESSEDIA structure and work packages:


WP1: Safety and Security Verification Methodologies
WP2: Integrated Verification Toolbox development
WP3: High-level models for software verification
WP5: Use-cases
WP4: Quality assurance and certification
WP6: Dissemination, Communication, Exploitation, Standardisation and Training
WP7: Project, Risk, and Innovation-Management

Technical Approach:

The VESSEDIA project is planned to run for 36 months. It is organized into seven work packages (WP) with significant dependencies and expected synergies between them which are described shortly in the following:

WP1: Safety and Security Verification Methodologies

This WP 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

WP2 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

The WP3 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

This WP 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

WP5 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

This WP 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

WP7 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.

Contacts:

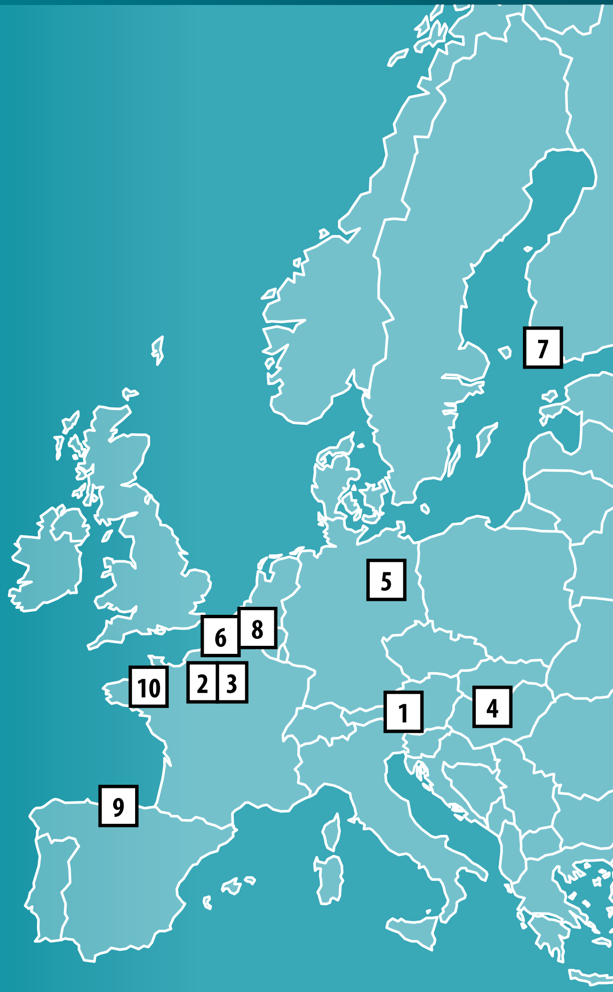
Project Coordinator:
Dr.-Ing. Klaus-Michael Koch
Technikon Forschungs- und
Planungsgesellschaft mbH
Burgplatz 3a
9500 Villach
Austria
Tel.: +43 4242 233 55
Email: coordination@vessedia.eu
Web: www.vessedia.eu

Technical Leader:
Dr. Armand Puccetti
Commissariat à l'énergie atomique et
aux énergies alternatives
DRT/LIST/DILS/LSL
F-91191 Gif Sur Yvette Cedex
France
Tel.: +33 169088304
Email: armand.puccetti@cea.fr

www.designation.at Foto: Depositphotos

Consortium:

The VESSEDIA consortium brings together a team of recognized partners in the fields of industry and research in combination with innovation-oriented SMEs and a certification expert. This makes it suitable to achieve the project's objectives. These 10 VESSEDIA partners are spread over 7 European countries and comprise basic research and service design with applied research and end-user oriented service. The complementarity of the partners' expertise aim at creating value for individual enterprises and institutions and their value chains.



Project Partners:

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

2 **Commissariat à l'énergie atomique et aux énergies alternatives, France [Saclay]**

3 **Dassault Aviation, France [Saint-Cloud]**

4 **Search-Lab Biztonsági Értékelo Elemzo és Kutató Laboratórium Korlátolt felelosségu társaság, Hungary [Budapest]**

5 **Fraunhofer Institute for Open Communication Systems FOKUS , Germany [Berlin]**

6 **Institut National de Recherche en Informatique et Automatique, France [Lille]**

7 **Turun Ammattikorkeakoulu Oy, Finland [Turku]**

8 **Katholieke Universiteit Leuven, Belgium [Leuven]**

9 **Fundación Deusto, Spain [Bilbao]**

10 **Amossys SAS, France [Rennes]**