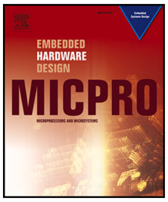
Contents lists available at ScienceDirect

Microprocessors and Microsystems

journal homepage: www.elsevier.com/locate/micpro



The VALU3S ECSEL project: Verification and validation of automated systems safety and security

J.A. Agirre [a], L. Etxeberria [a], R. Barbosa [b], S. Basagiannis [c], G. Giantamidis [c], T. Bauer [d], E. Ferrari [e], M. Labayen Esnaola [f], V. Orani [g], J. Öberg [h], D. Pereira [i], J. Proença [i], R. Schlick [j], A. Smrčka [k], W. Tiberti [l,*], S. Tonetta [m], M. Bozzano [m], A. Yazici [n], B. Sangchoolie [o]

[a] MGEP, Spain
[b] University of Coimbra, Portugal
[c] United Technologies Research Centre, Ireland
[d] Fraunhofer IESE, Germany
[e] Rulex Innovation Labs, Italy
[f] CAF SIGNALLING, Spain
[g] CNR-IEIIT, Italy
[h] KTH Royal Institute of Technology, Sweden
[i] CISTER/ISEP – P.Porto, Portugal
[j] AIT Austrian Institute of Technology, Austria
[k] Brno University of Technology, Czech Republic
[l] University of L'Aquila, Italy
[m] Fondazione Bruno Kessler, Italy
[n] Eskisehir Osmangazi University, Turkey
[o] RISE Research Institutes of Sweden, Sweden

ARTICLE INFO

Keywords:
Verification
Validation
Automated systems
Security
Privacy

ABSTRACT

Manufacturers of automated systems and their components have been allocating an enormous amount of time and effort in R&D activities, which led to the availability of prototypes demonstrating new capabilities as well as the introduction of such systems to the market within different domains. Manufacturers need to make sure that the systems function in the intended way and according to specifications. This is not a trivial task as system complexity rises dramatically the more integrated and interconnected these systems become with the addition of automated functionality and features to them. This effort translates into an overhead on the V&V (verification and validation) process making it time-consuming and costly. In this paper, we present VALU3S, an ECSEL JU (joint undertaking) project that aims to evaluate the state-of-the-art V&V methods and tools, and design a multi-domain framework to create a clear structure around the components and elements needed to conduct the V&V process. The main expected benefit of the framework is to reduce time and cost needed to verify and validate automated systems with respect to safety, cyber-security, and privacy requirements. This is done through identification and classification of evaluation methods, tools, environments and concepts for V&V of automated systems with respect to the mentioned requirements. VALU3S will provide guidelines to the V&V community including engineers and researchers on how the V&V of automated systems could be improved considering the cost, time and effort of conducting V&V processes. To this end, VALU3S brings together a consortium with partners from 10 different countries, amounting to a mix of 25 industrial partners, 6 leading research institutes, and 10 universities to reach the project goal.

1. Introduction

The main effort in the development of automated systems is placed on a key factor, which is *getting them to work*: as the new functionality of these automated systems was shown in development prototypes, they shall be introduced to the market. Between a prototype demonstrating new capabilities and a production version ready for the market, there are significant differences concerning quality attributes such as safety, cyber-security and privacy (SCP). The quality properties of a system

* Corresponding author.
E-mail address: walter.tiberti@univaq.it (W. Tiberti).

https://doi.org/10.1016/j.micpro.2021.104349
Received 2 February 2021; Received in revised form 4 June 2021; Accepted 9 June 2021
Available online 12 November 2021

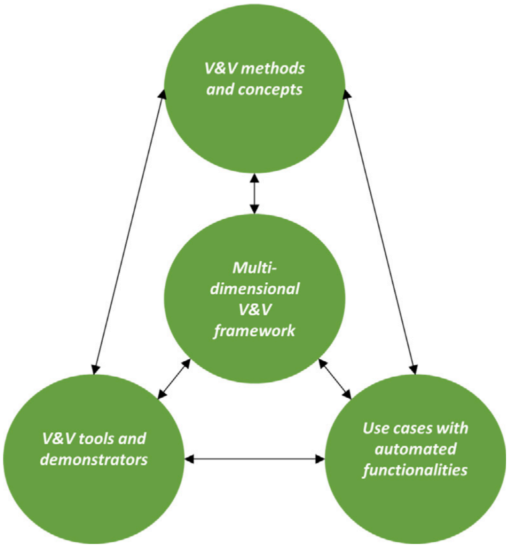

V&V methods and concepts
Multi-dimensional V&V framework
V&V tools and demonstrators
Use cases with automated functionalities

Fig. 1. VALU3S focuses on improving the V&V processes.

can be ensured through verification and validation procedures that take the respective requirements into account. V&V has become a strong procedure to protect a system against cyber-security attacks [1], as there has been a growing threat surface dealing with cyber–physical attacks [2,3]. As illustrated in Fig. 2, cyber–physical disasters have become common starting especially in 2005 to date affecting many sectors like automotive, health, etc. This shows that cyber-threats are not only affecting software assets anymore. Recently, cyber-security is being diversified with new techniques, making VALU3S' multidimensional framework (covering a wide spectrum of cyber–physical security and safety in leading sectors) a strong leverage for Europe's development in emerging areas mentioned in [4].

The focus of VALU3S [5] is on verification and validation (V&V) of cyber–physical automated systems. To this aim, VALU3S investigates methods, tools and concepts that are not only suitable for the evaluation of automated systems, but also improve time and costs of the V&V process. The project aims to create and evaluate a multi-domain verification and validation framework, which facilitates the evaluation of automated systems from component level to system level, with the aim of reducing the time and effort needed to evaluate these systems. In this way, we will provide practitioners with detailed information about all components involved in the V&V process. Such information is then used to facilitate the V&V process through the identification of V&V tools, concepts and processes used in different domains. In particular, the considered framework is multi-dimensional and multilayered (see Fig. 1).

The framework also facilitates a gap analysis within a domain to identify the concepts that go beyond the boundaries of a domain. The framework is then used as a major input to obtain the main objective of the project, which is design and development of V&V methods and tools that improve the time and cost of V&V processes.

The project started on May 1, 2020 and will last for three years. In this paper, we highlight the project goals, explain selected approaches, describe application domains, and discuss implementation issues.

2. Project objectives

VALU3S will cover V&V of automated systems in six different domains: automotive, agriculture, railway, healthcare, aerospace and industrial robotics. The high complexity of automated systems incurs an overhead on the V&V process making it time-consuming and costly. VALU3S aims to design, implement and evaluate state-of-the-art V&V methods and tools that reduce the time and cost needed to verify and validate automated systems with respect to SCP requirements. The objectives of this project are structured as follows:

(1) VALU3S will tackle SCP V&V for cyber–physical systems by creating a list of methods that is suitable for improving the time and cost of V&V processes. To do so, a V&V state-of-the-art analysis as well as a gap analysis will be conducted to identify commonly used V&V methods. The gap analysis facilitates the extension of VALU3S repository of V&V methods by identifying additional methods that take into account (i) methods that are defined specifically for automated system functionalities, (ii) methods that make use of research conducted on an individual component to argue about the SCP of multiple components, and (iii) combinations of methods that allow us to provide arguments and evidence for SCP of complex automated systems.
(2) The project will develop a multi-layered framework for more effective verification and validation of automated systems with respect to SCP requirements of the VALU3S scenarios.
(3) VALU3S will introduce a novel V&V workflow that is generic to reference methods in selected cyber–physical domains. This will then be complemented by the implementation of tools supporting the improved processes. In addition to the VALU3S repository of methods, the fulfilment of this objective is dependent on the VALU3S repository of scenarios, and detailed use case descriptions.
(4) In total, 13 use cases from 6 domains (Fig. 3) will be considered to demonstrate the strengths of the proposed methodology concerning both ensuring fulfilment of SCP requirements, and reduction of time and costs of V&V processes. For each of the target domains, VALU3S will conduct a survey on state-of-the-art scenarios useful for evaluating SCP requirements of automated systems. This will be used to test and validate scenarios for SCP evaluation of the proposed methodologies. To this purpose, the project will define evaluation criteria that include (i) metrics that are vital to measure system SCP within each domain under investigation, as well as (ii) the criteria that are used to measure the obtained V&V improvements such as test coverage, time and cost needed to conduct V&V using a specific tool.
(5) VALU3S will revisit and identify the weaknesses of relevant safety and security standards, and develop a concrete strategy to influence the development of new standards targeting SCP, an active participation in related standardization groups is considered. This is complemented via identification of gaps in different standards with regards to V&V methodology to conduct SCP-related V&V of automated systems.
(6) VALU3S will provide guidelines for end-users and practitioners to the testing community on how the V&V of automated systems could be improved by taking into account the time and cost of conducting the evaluations. The aim is to increase the awareness of the importance of conducting SCP V&V, and will be complemented through dissemination of project results, active involvement in scientific conferences and workshops, and frequent press releases.

2.1. Key Performance Indicator (KPI)

These are the KPIs defined in VALU3S for a quantifiable measure of performance over time for project specific objectives:

(1) Improve at least 13 V&V methods in order to create the VALU3S repository of improved V&V methods.
(2) Create at least a 6-dimensional V&V framework and detail the layers of the dimensions.
(3) Develop at least 13 novel tailored V&V workflows that will improve the time and cost of V&V processes.

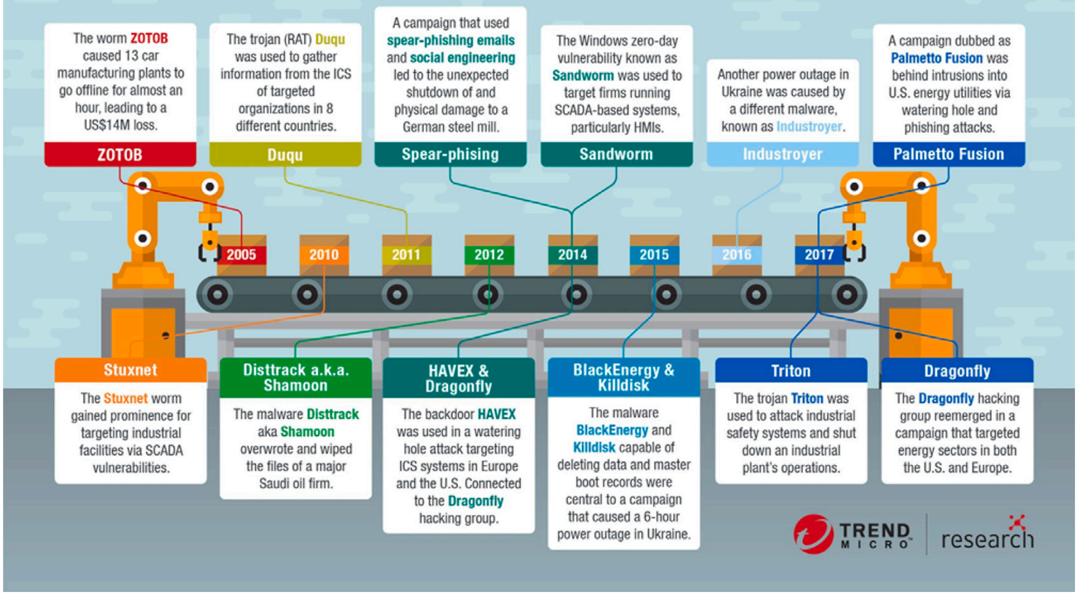

The worm ZOTOB caused 13 car manufacturing plants to go offline for almost an hour, leading to a US$14M loss.
ZOTOB
The trojan (RAT) Duqu was used to gather information from the ICS of targeted organizations in 8 different countries.
Duqu
A campaign that used spear-phishing emails and social engineering led to the unexpected shutdown of and physical damage to a German steel mill.
Spear-phising
The Windows zero-day vulnerability known as Sandworm was used to target firms running SCADA-based systems, particularly HMIs.
Sandworm
Another power outage in Ukraine was caused by a different malware, known as Industroyer.
Industroyer
A campaign dubbed as Palmetto Fusion was behind intrusions into U.S. energy utilities via watering hole and phishing attacks.
Palmetto Fusion
2005
2010
2011
2012
2014
2015
2016
2017
Stuxnet
The Stuxnet worm gained prominence for targeting industrial facilities via SCADA vulnerabilities.
Disttrack a.k.a. Shamoon
The malware Disttrack aka Shamoon overwrote and wiped the files of a major Saudi oil firm.
HAVEX & Dragonfly
The backdoor HAVEX was used in a watering hole attack targeting ICS systems in Europe and the U.S. Connected to the Dragonfly hacking group.
BlackEnergy & Killdisk
The malware BlackEnergy and Killdisk capable of deleting data and master boot records were central to a campaign that caused a 6-hour power outage in Ukraine.
Triton
The trojan Triton was used to attack industrial safety systems and shut down an industrial plant's operations.
Dragonfly
The Dragonfly hacking group reemerged in a campaign that targeted energy sectors in both the U.S. and Europe.
TREND MICRO
research

Fig. 2. Evolution of security threats and risks over the past decades [6].

Fig. 3. VALU3S target research domains.

(4) Prove the concept of improved V&V processes by applying the improved V&V methods and tools to 13 use cases covering the 6 top-priority domains listed in ECS (Electronic Components and Systems) Strategy Research Agenda-2018 [7].

(5) Present and detail at least 13 novel evaluation scenarios (including their requirement specifications) for safety, security and privacy evaluation through 13 realistic use cases.

(6) Improve and/or develop at least 24 V&V tools that aim to improve the time and cost of V&V processes while dealing with hardware-, software- and system-level cyber–physical risks.

(7) Incorporate and make use of at least 13 SCP evaluation criteria as well as at least 11 evaluation criteria suitable for measuring the level of improvement obtained in the V&V processes.

(8) Conduct a comprehensive gap analysis on SCP V&V methods, tools and concepts detailing strengths and weaknesses of the existing standards through active participation in at least 14 standardization initiatives which are also used as platforms to disseminate the results of VALU3S.

(9) Release 6 newsletters in addition to continuous updating and reporting of dissemination activities. Moreover, VALU3S partners aim to disseminate the project results through publication of at least 45 scientific articles.

3. Concept and methodology

3.1. Concept

In the VALU3S project, we focus on 6 domains, studying a total of 13 use cases, described in Section 5, that are semi or fully automated. Alongside manufacturers of the automated systems, manufacturers of microprocessors, sensors, robotic arms, cameras, RADARs (RAdio Detection And Ranging), LIDARs (LIght Detection And Ranging) and SONARs (Sound Navigation And Ranging) as well as developers of image processing and machine learning algorithms [8,9] are other actors that play a vital role in the process of designing and implementing automated systems.

As the functionalities of automated systems have been shown in development prototypes, they need to be introduced to the market. However, between a development prototype demonstrating new capabilities, and a production version, there are significant differences with respect to safety and reliability. In other words, manufacturers of these systems need to make sure that the systems work in the intended way and according to specifications. This is not a trivial task as system complexity rises dramatically with the increase of automated functionality being added to these systems. With rising complexity, unknown properties of systems under development may emerge during the integration of components on different levels (e.g., hardware, software) making it necessary to conduct verification and validation of these systems before making them available to the market, to provide safe, secure and reliable systems for society.

The high complexity of automated systems also incurs an overhead on the V&V process making it time-consuming and costly. This is where the VALU3S project comes into the picture: it aims to combine and enhance state-of-the-art V&V methods to reduce the time and cost needed to verify and validate automated systems with respect to SCP requirements. To this end, we will design a multi-domain framework and evaluate it with the aim to create a clear structure around the components and elements needed to conduct V&V process through

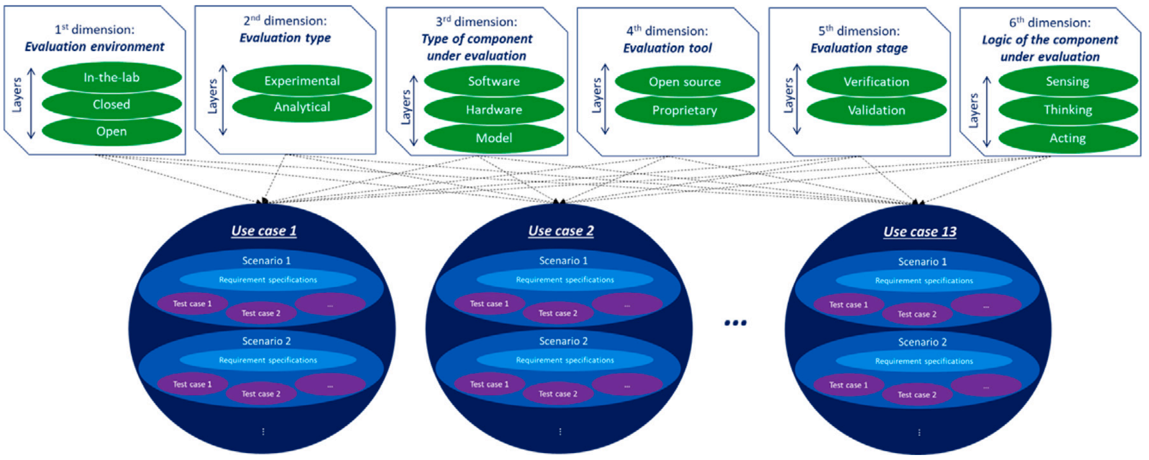

1st dimension: Evaluation environment
Layers
In-the-lab
Closed
Open
2nd dimension: Evaluation type
Layers
Experimental
Analytical
3rd dimension: Type of component under evaluation
Layers
Software
Hardware
Model
4th dimension: Evaluation tool
Layers
Open source
Proprietary
5th dimension: Evaluation stage
Layers
Verification
Validation
6th dimension: Logic of the component under evaluation
Layers
Sensing
Thinking
Acting
Use case 1
Scenario 1
Requirement specifications
Test case 1
Test case 2
...
Scenario 2
Requirement specifications
Test case 1
Test case 2
...
Use case 2
Use case 13
...

Fig. 4. VALU3S initial multi-dimensional layered framework.

identification and classification of evaluation methods, tools, environments and concepts that are needed to verify and validate automated systems with respect to SCP requirements.

The framework (the initial version of the framework is illustrated in Fig. 4) is multi-dimensional as it identifies several properties that facilitate the V&V of automated systems, and maps each of these properties to the use cases under analysis.

As shown in Fig. 4, the framework is also layered, since the evaluation process could be detailed with multiple alternatives to choose from in each of the dimensions. For example, the evaluation stage is layered into (i) verification and (ii) validation. Note that this is an initial attempt to identify different elements of the framework.

The framework, as whole, will target a level of automation up to level 3, i.e., it will provide a list of suitable V&V methods and suggestions which users can view and adopt. Indeed, the framework is planned to be further elaborated in the course of the project as part of the work done in WP2, as will be detailed in Section 6.

The multi-dimensional framework and its web-repository will be made available as part of the final project output and will be possible to update with new V&V methods and tools.

3.2. Methodology

As already stated, the main goal of the VALU3S project is to reduce time and cost of V&V in semi and fully automated systems through the design and implementation of a set of process workflows and tools resulting from an investigation of existing methods, tools, and concepts, which are suitable for the evaluation of these systems. The VALU3S methodology consists of a four-step-process described in the remainder of this section.

(1) ***Instantiation of use cases and creation of VALU3S repository of evaluation scenarios.*** To verify and validate a system we need to define detailed test cases as well as requirement specifications about different situations where the use cases should be evaluated in. These test cases are then used as a basis of the V&V process, where the evaluation of the results of the execution of these test cases provides evidence about whether the system under test is safe and secure. It is challenging to generate appropriate test cases, which are also representative of real-world scenarios. This can significantly contribute to the time, cost and effort of the V&V process. To do this, we plan to conduct interviews with stakeholders in different domains to identify commonly-used scenarios, and create a VALU3S repository of scenarios. The repository will also contain scenarios designed and proposed by VALU3S partners as a result of the identified gap between the commonly-used scenarios and the need of the domains; We also plan to conduct a commonality evaluation of the use cases instantiated as well as VALU3S repository of scenarios. This way, we can identify common points between use cases and scenarios as well as grouping the requirements of different domains.

(2) ***Creation of VALU3S repository of V&V methods.*** We plan to create a VALU3S reference method list to be used for the V&V of automated systems. The reference methods will then be used in the third step to implement a set of process workflows and tools to reduce time, cost and effort needed in the V&V process. To this end, we plan to conduct an analysis of the commonly-used and state-of-the-art experimental and analytical V&V methods (such as fault and attack injection [10]) within each of the domains useful for evaluating the SCP requirements of automated systems. Through an analysis of the commonly-used V&V methods, we will be able to identify the gap between the methods that are available, and the ones that are needed for the evaluation of automated systems. The VALU3S reference method list would then contain the commonly-used methods as well as (i) methods that are improved and (ii) new methods that are created by a combination of existing and newly developed methods;

(3) ***Design and implementation of a set of tailored process workflows and tools to improve the time and cost of V&V process.*** We plan to design and implement a set of process workflows and tool chains to improve time and cost of the V&V of automated systems. Several tailored process workflows have been identified and will be investigated throughout the project. The design of these process workflows requires detailed information about the scenarios (step 1) as well as a repository of V&V methods (step 2), which are accompanied by information about different components and subsystems needed within each environment to verify and validate scenarios provided by different layers of the V&V framework;

(4) ***Evaluation of the tailored process workflows and tools.*** The final step of the methodology corresponds to the evaluation of the process workflows and tools that were designed and implemented in step 3. To do so, we need to create and detail a set of evaluation criteria to conduct measurement and quantification of the SCP requirements as well as comparing time and cost efficiency of the tailored V&V workflows and tools. The evaluation of the tailored process workflows and tools will be conducted in a set of demonstrators.

4. Beyond the state of the art

4.1. Overview

V&V is one of the most important activities in the development of cyber–physical automated systems. Developing software that meets SCP requirements for those applications is a formidable task. With new political and market pressures to deliver more software at a lower cost, optimization of their methods and standards need to be investigated. The industry must follow standards that strictly set quality goals and prescribes engineering processes and methods to fulfil them. V&V is therefore a time-consuming task in front of the dynamic behaviour and architectures of cyber–physical automated systems, which are not necessarily known at design-time [10–13].

This section deals with topics that constitute a significant advance over the state of the art in V&V. As state in objective 1 (multi-layered framework), VALU3S addresses the V&V of various dependability concerns with special focus on SCP requirements and aims at advancing the state of the art across multiple disciplines. One of the most promising is aspects here is the application of artificial intelligence (AI) and machine learning (ML) technologies to V&V and to understand how data-driven testing can accelerate the V&V process. However, VALU3S will also look at other more established design approaches (model-based safety, run-time verification, risk assessment, continuous architectural design and automation of testing topics) and how they may be interfaced with new hardware and software architectures (e.g., Digital Twin and Fault and attack injection topics). Many of them exploit AI as well, thus investigating how model-based and data-driven testing can work together. Moreover, as the final aim of VALU3S is to fill the gap between research and the market, specific topics address new platforms for V&V (robotics, driving simulator, teleoperation and surveillance).

4.2. Machine learning

In the last 15 years, the research in the field of security for CPS has focused on the study of external attacks and anomalies which can affect the system [2]. Hence, one of the main goals of CPSs security is to detect and isolate such attacks and anomalies, often referred to as failures. In previous years, a lot of effort has been spent in the development of Fault Detection and Identification (FDI) algorithms to unveil system's failures. In particular, model-based approaches started in the 70's, with the pioneering works [14,15] on observer-based FDI, and evolved from the 80's [16] to date [17–19]. However, one of the problems that arise when dealing with complex systems, e.g. automotive systems, industrial plants, etc., is that deriving a physics-based model can be burdensome or even prohibitive, as for example in the case of complex buildings modelling [20]. For this reason, in the last years researchers started to investigate new approaches that are based on the use of data, and that leverage Machine Learning (ML) techniques to create the so-called data-driven models [20]. This is possible thanks to the increasing use of the new technologies that allows to both easily collect large amounts of data and to implement data-driven algorithms in an efficient way.

In order to have clearer understanding on how the main features that AI and machine learning approaches, mechanisms and tools can be adopted in VALU3S activities, and how these can support the development of improved V&V solutions, we are investigating on representative sets of data- and behaviour-related system characteristics. We will map the challenges related to those characteristics to the project's objectives, in particular, in the application domains where solving these challenges can bring improvements over baseline V&V solutions.

4.3. Digital Twins

In Industry 4.0 all decisions on the business system optimize based on real time information from vehicles, robots, systems, components and people. Although there exist some frameworks to support efforts towards industry 4.0 [21,22], building and automation of these systems is still expensive and difficult. According to Industry 4.0, modelling (with *Digital Twins*) plays a key role in managing the increasing complexity of technological systems. A holistic engineering approach is required to span the different technical disciplines and prove end-to-end engineering across the entire value chain.

In most of the platforms providing Digital Twins simulators (such as EHUB, FlexSim, SIMUL8, Arena Simulation, Process Simulator, TaraVRbuilder etc.), SCP are still the weakest component as such systems are still subject to cyber–physical attacks. In VALU3S we will adopt effective fault injection and cyber prevention mechanisms that may protect the digital twins and the physical infrastructures of industry 4.0 factories. Among other techniques, virtual prototypes are a natural candidate for such type of verification.

4.4. Failure Detection and Diagnosis

There exist different types of Fault Detection and Diagnosis (FDD) approaches that are applicable to robotic systems. Likewise, in the industrial robotics domain, faults have the potential to affect the efficiency of the underlying process, namely causing failures of internal physical components (e.g., robot, IPC, sensors, actuators), or even compromising the safety of humans interacting with the robot. Concurrently, when detecting a fault, usually a diagnosis process is induced in order to identify which internal components are involved. It should however be noted that applying FDD for industrial robotics is a relatively new approach. On the one hand, there exists a wide spectrum of different types of industrial robots, and on the other hand there exist different FDD approaches such as data-driven, model-based, and knowledge-based approaches [23]. Data-driven approaches for instance are based on near real-time process data with the aim of statistically differentiating a potential fault from historical data, e.g., via clustering techniques such as Principle Component Analysis (PCA). Model-based approaches use analytical redundancy to detect and diagnose faults, while knowledge-based approaches typically associate recognized behaviours with predefined known faults and diagnoses. Analytical or stochastic a priori models are particularly used in respect to internal sensors of a robotic system when the system operates in a well-known work environment. For robotic systems operating in unknown environments, data-driven approaches are the better choice by applying sensor fusion techniques for external sensor fault detection. This means that multiple sensors sense different aspects of the environment (e.g. orientation and location), while their readings can be fused to form a consensus. Sensor-fusion-based fault detection approaches for robotic systems include different algorithms such as: Kalman filters, Dempster–Shafer, correlation and distribution-based, and Bayesian networks. Relying on data-driven approaches, fault injection and supervised learning induce expressions that are sensed by the external sensors and form the basis of creating training data sets.

There exists a deficit for using FDD approaches (particularly data-driven approaches) that are dedicated to detecting and diagnosing faults related to interactions between robots and humans (HRI). Furthermore, HRI are subject to uncertainty due to the fact that unexpected outcomes might lead to unknown faults and failed interactions. VALU3S will go beyond the state-of-the-art by applying FDD approaches to an HRI semi-automated assembly scenario. Also the detection of unknown faults while distinguishing between failed interactions, that resulted from internal faults and failed interactions that resulted from external events, will be considered in VALU3S. Particularly in situations where faults might occur that were not seen before, the application of unsupervised machine learning approaches will be investigated complimentarily to the proposed supervised learning. The state of the art in FDD shall further be advanced by managing interaction-related faults between humans and robots, as humans may have the tendency to compensate for a faulty behaviour of a robot during interaction. Therefore, the envisaged industrial robotic use case considers (next to other external sensors of the HRI workplace) the behaviour and actions of the human as well by capturing the human movements with a 3D-shape sensor system, with the aim of detecting potential fault-preventing behaviours of humans, or for diagnosing the reason for a failed interaction with the robot.

4.5. Hardware-based solutions for cyber–physical and IoT security

CPSs have become commonly used in critical infrastructures, mainly in the context of power grids [24,25] and industrial systems [26]. Besides very general examples like the infamous Stuxnet attack [27], also several risks in different contexts have been identified [28], as well as corresponding methods, i.e. in the field of machine learning [29].

In VALU3S, we aim to improve existing hardware-based security solutions, in particular, we aim to replace *Physical Unclonable Functions* (PUF) solutions with *True-Random Number Generators* (TRNG). The concept of a PUF was proposed in 2001 as a physical one-way function. Since then the concept has been explored for practical circuits to enhance security. PUFs are meant to complement or replace other hardware authentication techniques such as biometric authentication, smart cards and hardware one-time password (OTP) tokens. OTP tokens and smart cards can be either replaced or complemented by PUFs. PUFs and TRNGs can be implemented by similar architectures. PUFs can generate unique single random numbers whereas TRNGs can continuously generate random numbers that can be used as cryptographic keys, padding bytes, blinding values, nonces, etc. The alternative is the hardware-based TRNGs which will be used in VALU3S. Hardware-based security by TRNGs will be adapted to industrial applications enabling a low-level solution against cyber–physical attacks. Here, an industrial FPGA-based very fast TRNG will be developed to create OTPs for device authentication which is indispensable in industrial IoT.

4.6. Model-based safety analysis

In recent years, there has been a growing industrial interest in model-based safety assessment techniques (MBSA) [30–32] and their application. These methods are based on a single safety model of a system, and analyses are carried out with a high degree of automation, thus reducing the most tedious and error-prone activities that today are performed manually. Formal verification tools based on model checking have been extended to automate the generation of artefacts such as Fault Trees and FMEA tables, which are required for certification of safety critical systems [33,34]. A distinguishing feature of some existing approaches to MBSA is the possibility to automatically inject faulty behaviours into a behavioural model, based on fault specifications taken from a fault library. In this view, the behavioural model of a given system, called nominal model, is augmented with the faults to be injected, yielding the so-called extended model. The extended model can then be processed by model checking engines to generate Fault Trees and FMEA tables.

Existing tools that support MBSA via fault injection include the xSAP safety analysis platform [35]. xSAP is a generic platform for MBSA, which provides a variety of features. It enables the definition of fault modes, based on a customizable fault library and automatic fault injection. Moreover, it implements a full range of safety analysis techniques, including FTA, FMEA, failure propagation analysis and Common Cause Analysis (CCA). Finally, XSAP implements a family of effective routines for such analyses, based on state- of-the-art model checking techniques, including BDD-, SAT- and SMT-based techniques. Automated fault injection techniques will be extended and tailored to the different testing layers identified in the project, guided by use cases. The fault library will be extended accordingly, to encompass fault types needed to deal with fault cases. Techniques and tools for MBSA such as the xSAP tool will be further engineered to address use case needs, to address potential scalability issues, and to provide support for certification activities.

4.7. Model checking of controller design

V&V of the controller design of automated systems is a fundamental problem to ensure SCP requirements. Control software is often derived from simulation models, which in turn are derived from control theory models such as dynamical systems. A fundamental step in the verification and validation of control software for complex cyber–physical systems is the analysis of the interaction with the controlled physical plant. Such interaction can be formally represented by hybrid systems, which combine discrete state transitions with continuous dynamics equations. There exist several model checking techniques and tools specialized for hybrid systems. These tools are mainly focused on the verification of invariants and most of them compute an over-approximation of the set of the reachable states. HyTech [36] is a model checker for linear hybrid automata, which represents the continuous part of the reachable states using polyhedra. Phaver [37] and SpaceEx [38] verify affine continuous dynamics with inputs. Other model checkers such as HSolver [39], d/dt [40] and Flow* [41] verify invariants of non-linear hybrid systems. KeYmaera [42] is a theorem prover for hybrid systems that can handle non-linear hybrid systems, with symbolic parameters and an unbounded number of components. Other tools such as HyCOMP [43] and HybridSAL [44] are based on SMT-based model checking and encode linear hybrid systems as infinite state transition systems and apply various abstraction techniques.

Despite the availability of so many tools, the scalability and applicability of automated and exhaustive verification techniques such as model checking are quite challenging due to the complexity of the dynamics used to model control assumptions on the physical parts of the system. VALU3S will consider software model checking and hybrid systems model checking techniques, as well as their interplay, to overcome limitations of the current approaches to formal verification of these systems. Scalability issues of current model checking techniques will be addressed by investigating new abstraction techniques. In particular, algebraic decomposition [45] and implicit predicate abstraction [46] will be combined to verify hybrid systems with complex dynamics.

4.8. Monitoring actions to support run-time verification

A software monitoring solution is based on the exploitation of the processors that are executing the application under examination to collect data useful for monitoring. For example, the execution time estimation of a task could be done in two possible manners: activating a timer (if available in the system) at the start of the task and then stop it when the task ends or generating interrupts in order to sample internal state of the system (i.e., the program counter). There are various examples of software based profiling systems, that depend on the application [47–51]. Hardware monitoring systems are based on dedicated hardware resources able to carry out the profiling action. This means that no source code instrumentation is needed and the software execution by the central processor unit is not altered, thus no overhead on execution time is introduced. For the same reason, hardware solutions can guarantee the best accuracy in performance analysis. However, these solutions require a larger silicon area occupation for system implementation and it is difficult to correlate low-level measurements to source code performance metrics and the limited number of allocable hardware resources. This often forces the collection of desired performance metrics by means of multiple tests. Various examples of hardware-based profiling approaches have been presented in literature [52,53]. To summarize, characteristics of hardware solutions are, i. No execution overhead, ii. Bigger area occupation, iii. Bigger power dissipation, iv. Difficulty to correlate low-level measures with source code information, and v. Redesign to be ported among different architectures. Characteristics of software solutions are i. Execution overhead, ii. Portable among different architectures, and iii. More occupied memory for data.

In VALU3S, the proposed research solution in the context of monitoring focuses on different points. The first is the possibility to tailor and customize the monitoring system for the system under examination: it depends on when to use the monitoring action (i.e. during the lifecycle to characterize the system or during development phases to support the designer); and it depends on the platform selected for the system (ASIC, reconfigurable logic). Other considerations should be done referring to non-functional properties of the system itself (how much overhead can be inserted, if a real-time profiling action is requested, etc.). The second is the development of a framework able to support the designer in the selection of a profiling solution. The third is to integrate this framework with support to provide the best instrumentation policy starting from design requirements. The fourth is to execute parts of the system within a simulated environment. Such setup becomes necessary as the systems become bigger and bigger, where the goal is to verify the interaction of a new component with simulated existing system parts.

4.9. Wireless Sensor Networks security

Wireless Sensor Networks (WSNs) are versatile and distributed sensing systems that are conceived to support a wide variety of application domains, such as environmental surveillance [54], building automation, localization [55], health monitoring, intelligent transportations [56]. Typically, a WSN consists of a large set of sensor nodes, i.e. tiny, low-cost and battery-powered devices with constrained system (energy, computation, memory, and communication) resources that are able to self-organize as an ad-hoc network. Relying on WSNs for applications requires the commitment to develop SW applications for such systems [57]. This might be very challenging, especially when exploiting only traditional development platforms [58]. As a consequence, in recent years a lot of effort has been devoted to investigating the exploitation of middleware as extended platforms for developing WSN applications. Despite the several proposals available in the technical literature, security is not usually included in the services portfolio provided by middleware platforms. Nevertheless, especially when considering WSN applications in the “control and monitoring” domain, one of the most important issues is to ensure data and system reliability, and reliability strictly involves security issues [59,60]. In this regard it is worth noting that even if many network standards, like IEEE 802.15.4, provide some basic security facilities, the integration with other vendor-specific mechanisms, such as the cryptographic keys generation and management scheme [61] to feed the codec or the party authentication logic, is mandatory for their effective practical adoption. Moreover, the network layered architecture suggests that security services should be implemented across multiple layers of the protocol stack. In particular, a cross-layer design would enable efficient and coordinated attack defence strategies and security services for each protocol layer. However, security-oriented middleware for WSNs often focuses only on cryptography [62–64].

One of the ambition in the project is to integrate in the whole architecture a middleware for WSNs that provides network security in terms of all its relevant aspects: data confidentiality, data integrity, data authenticity, and system availability. The goal is the prevention of passive attacks on data through cryptography and also detection of active attacks against network availability. Specifically, the services provided by such a middleware will be: Party authentication service; Key generation and management service using WSN-specific mechanisms [65,66]; Intrusion detection and threat estimation service [67,68]. The middleware and its services will improve the V&V processes by providing enhanced V&V methods (e.g., WPM-based IDS [66]) to check and to satisfy the SCP requirements in WSNs platforms. The middleware will be mainly tailored to real-world IEEE 802.15.4-based WSNs and also to other kind of resource-constrained network (e.g. MANET) exploited in the project.

4.10. A-priori and online Risk Assessment for automated systems

In recent decades, the electronic systems used in the most varied applications have undergone a double revolution: they have become increasingly autonomous, therefore able to perform even complicated functions without human intervention. And a network of interconnected systems (Internet of Things) able to communicate remotely, exchange information and make decisions based on them was created. Since the nature of these systems is becoming very complex, it is a challenging task to enable quality assurance, especially satisfying a high level of safety and security towards the system itself, but also to protect the surrounding environment, human beings and assets from undesired losses. In this context, Risk Assessment could be a useful tool to identify potential threats, evaluate the likelihood and the consequent impact, giving the stakeholder a chance to define effective countermeasures and mitigation strategies. To perform this assessment, several methodologies have been identified [69]; the most common are HAZOP [70], FTA [71], STAMP [72] and ETA [73]. However, none of them represents a completely valid and comprehensive solution to deeply analyse all the possible issues in such a complex, dynamic and interconnected system.

In VALU3S, an ad-hoc Risk Assessment tool for Automated Systems will be developed starting from current methodologies. This tool will a-priori be able to evaluate the level of risk of system operations in a comprehensive and exhaustive manner, considering several aspects such as: environment conditions, presence of humans, communication between devices, data management and protection, cybersecurity, physical threats, electronic and mechanical faults, etc. Furthermore, the RA tool will also be suitable to be applied during system operations, in order to dynamically assess the most likely and dangerous threats and give the chance to the operator to immediately react applying real-time safety countermeasures (e.g. change the parameters of the scheduled operations or eventually stop them).

4.11. Continuous simulated evaluation of architectural design of software-intensive systems

In today’s extensively dynamic software systems, there is a strong requirement of continuous introduction of new features. Continuous software engineering aims to deal with the rapid changes within the software-based ecosystems [74]. Continuous engineering considers business strategy, development, and operations. Business strategy [75] considers continuous planning and budgeting that evolve in response to changes in the business environment. Continuous development [76,77] considers areas such as integration, delivery, deployment, verification [78,79], compliance, and continuous architecting [80–82]. Our focus is on the continuous integration, verification, and architecting.

For the verification of individual components of a system, as well as the interaction between components of a system, there is a need to focus on the external behaviour of components. A simple “gut feeling” in complex system is not a relevant quantification approach. Instead, architects need to make decisions based on facts. In order to do so, in VALU3S we aim to extend the existing, state-of-the-art, architecture simulation approaches to support continuous verification of architectural decisions. Verification of the architectural decisions and the architectural design, in a simulated environment, shall be used for guiding the process of system architecting.

4.12. Medical robotics

The certification of Medical Devices in compliance with current regulatory requirements is a critical aspect in medical robotics. In VALU3S, we aim to move a step further to support the certification of medical devices. The inclusion of some new steps and tools to support new engineering methods is required in order to detect the fulfilment of compliance with requirements at earlier stages of development. The new product must be designed to a high safety/security/performance level compared with previous products developed by the company. Approaches to address this include early analysis of the impact of changed requirements, and coordinating the analysis of security, safety and performance requirements. The test bench platform to be developed in VALU3S will provide the means to cost-effectively develop a medical device that incorporates the monitoring functionality together with the control algorithm.

VALU3S will lead to significant advancements in the state of the art and practice on compliance for medical devices in particular in the research line of tasks automation by anaesthesiologists in the Operating Room. The goal in this use case will be to make the execution of these activities more efficient and at the same time more effective, with earlier detection of either technical/medical risks and emphasis on ergonomy based on human factors analysis. These advancements will result in medical devices that are more trustworthy overall, can be assured more rigorously and at lower costs, and have a shorter time to market. Additional ground-breaking innovative nature of the project lies in determining if existing cross-domain approaches are a good basis to conduct medical device development along the different project life cycles stages. VALU3S' use case on Vital Signs Controller by means of Drug Infusion is, by itself, a technological break-through in robotics and automation of tasks within the operating room. One of the objectives in VALU3S is to develop a Hardware-in-the-Loop Test-Bench Platform that will allow the system to be verified under laboratory conditions, by simulating the patient's response to the drug-dose infusion.

4.13. Driving simulator

Automated and connected vehicles have been rapidly developed during the past decades. These vehicles will play important roles in future transport systems. Up to now, they were usually limited to bounded, protected and predictable environments. Many aspects of such automated vehicles still need to be successfully verified and validated before they can be used on public roads. Conducting V&V on simulation level using advanced driving simulators is our main contribution to the state of the art, as simulation is a cost-efficient and risk-free alternative. An advantage of using driving simulators is that the whole vehicle-under-test is modelled (as opposed to having a detailed model of just one component or a subsystem, which is typically validated out of context). Therefore, using simulators, we can verify and validate the whole vehicle systems, and analyse how faults in components propagate through the whole system. Furthermore, we can analyse the impact on the traffic system level by using a simulation framework such as the one proposed in [83], combining a driving simulator with traffic simulators and network simulators (for simulation of V2X communication) such as SUMO [84] and Veins [85], respectively.

In VALU3S, the ambition is to create a methodology for applying V&V processes in simulation environments for advanced driving simulators. The proposed methodology should also validate whether the assumption(s) made during validation of each element still holds for the system level and will use propagation analysis to do so Moreover, with the driving simulators, drivers can be added into the V&V loop. Involvement of human drivers/operators in V&V processes is not commonly considered yet, but we expect this to be an important aspect of V&V of future vehicles and transport systems.

4.14. Teleoperation

Self-driving cars are recently a very popular and important topic. Several applications of self-driving vehicles can also be fulfilled with teleoperated cars. Some problems of fully autonomous vehicles can be mitigated by interventions of a human operator who is not sitting in the car, at the cost of introducing other challenges, like latency of the control and observation signals. Big players in the car industry such as Waymo, General Motors' Cruise, Nutonomy, Zoox, Drive.ai, Uber, and Nissan are most likely developing teleoperation systems. Since this domain is not publicly open and protected by company policies, it is not easy to obtain schematic details. There are also producers such as Caterpillar [86], Wenco [87], Sandvik [88], etc., who focus on remotely controlled vehicles working outside of the public infrastructure such as mining or agriculture machines, but also their schematics are mostly classified or incomplete. Generally, for both kind of manufacturers from the technological point of view the key issue of the system is latency: Remotely controlling a car does not work if latency is measured in seconds. Teleoperation systems can be operated through plugging into mobile networks using cellular radios. On a 4G connection with proper adjustments, latency times can fall below 100 ms. Moreover, some producers design dynamic solutions such as adjusting the resolution of the operator's video feed when the connection slows down [89]. The actual setup for the remote driver still evolves, but most of the producers use the feeds from various cameras on the car, a map of the area combined with GPS feed etc. To enable the teleoperation solution in general for public use, it is required to use a certain degree of safety and security. Conducting V&V especially of publicly accessible components of the teleoperation system, which is in this case a mobile network, is crucial to achieve this.

We plan to develop (and use) the VALU3S testing framework to examine and reduce the safety risks originating from the publicly used components of the system, especially focusing on the variable availability of the LTE network and possible latencies there. Based on the outcomes of the VALU3S testing framework, new safety features can be developed into the teleoperation and control modules to mitigate safety risks in remotely controlled cars.

4.15. Safety function out-of-context

Design, Test and Certification of safety-critical system components that are integral parts of system of systems are challenging and costly tasks. Connecting systems together in a chain increases the risk of cascade faults, which means that each individual system component must be designed at an extremely high safety-level so that the combined system achieves the required MTBF (mean-time between failure) that the safety standard dictates for the industrial domain in question. Further, the safety standards often demand the use of dual or triple channels to achieve the required safety level through redundancy or diversity. Currently, FPGAs are not used much in safety-critical systems, partly because of their susceptibility to soft-errors (e.g., data has been corrupted but the circuitry is still completely functional), but partly also because integrating many components in the same chip contradicts the way voltage diversity is treated in the calculations of MTBF in the safety standards. The voltage supply becomes a single point of failure. Thus, if the chip loses its power supply, both functions will disappear. The latter issue situation is usually alleviated by providing a dual backup for delivering voltage. To reduce the FPGAs susceptibility for soft-errors, the configuration memory of the FPGA needs to be scrubbed regularly to correct any single-event upsets that have occurred. This is done by instantiating a SEM core (Soft-Error Mitigation) on the FPGA. The SEM-core can fix single bit flips and detect multiple faults. An alternative technique for restoring functionality is Run-Time Reconfiguration (RTR) of the FPGA. Further, a SEM core can be used to inject faults in the configuration memory during run-time, which allows to partly perform the tests required by the certification process.

In VALU3S, we will implement a typical industrial safety-critical function to see how SEM cores in a Healing Core configuration [90] and the test/fault-injection methods behave in an industrial-like setting and how it affects the up-time, robustness and availability of the safe component. The idea is to detect the error using redundancy, and then repair the faulty sub-system component during run-time, before the safe functionality of the system is compromised. We will further determine how the fault manifests on the next level in the system hierarchy and create fault-models thereof for system simulation.

4.16. Intelligent Traffic Surveillance

In case of the Traffic Surveillance domain, systems are often very complex and consist of various components, often distributed over a site or even located at distant places (e.g., cameras. IR flashers, radars, other sensors, networking HW, servers, etc.). The systems are mostly not designed from scratch but reuse some existing solutions and often add some HW (or sometimes SW) for desired new functionality. In the case of such complex systems, the early adoption of V&V methods and tools, from the first phases of development process [91–93], is crucial.

Using the VALU3S V&V framework, the reliability and security of systems can be ensured before deployment of the systems to the field and thus catch most of the bugs introduced to the systems during design or redesign phases. This will sure result in reduced costs and reduce effort spent on system maintenance and bug-fixing after installation.

4.17. SCP test case automatic generation and execution

Manual test design, despite being the main technique in use for creating test definitions, is a lengthy, resource-intensive and error-prone task. The created test cases shall demonstrate that the implementation under evaluation conforms to the expectations, requirements and specifications. For software it is common to produce tests that have a certain coverage, either data flow, control flow or mutation coverage. Mutation coverage means that the tests can discover a number of small faults artificially inserted into the program. Coverage analysis ensures the quality of the tests in the sense that all implemented functionality is tested, but it does not ensure that the tests cover all the required functionality correctly. Since the requirements and specification exist typically only in prose and are interpreted by the engineers, they cannot be used directly to automate test design. Model-based testing formalizes the requirements into a model — this is usually easier and especially better maintainable than going directly to tests. From the model, tests can be automatically derived.

In VALU3S, we intend to expand model-based testing in two interesting, novel ways. One is to marry fault injection with model-based mutation testing. Thereby we will be able to show the robustness of the system by testing whether a fault propagates, to quantify which types of faults are more severe than others and to optimize fault-injection experiments. The other is automatically de-factoring in models. A development team could choose different ways to distribute information and functionality in the code, compared to the model. This can be mimicked by automatically transforming (de-factoring) the model into multiple variants before using it for model-based testing.

4.18. Fault and attack injection

Fault injection is a testing method used to accelerate the occurrences of faults for evaluating fault tolerance and thereby system safety. Analogous to fault injection, attack injection may be used to evaluate the impact of cyber-security attacks on system security [10,94,95]. This is due to the fact that cyber-security attacks may be considered as a special type of faults which are human made, deliberate and malicious, affecting hardware/software from external system boundaries and occurring during the operational phase [96]. Security testing may be conducted using fuzz testing, vulnerability testing and penetration testing [97]. Fuzz testing may be performed by fault injection focused on the system input to investigate the effects of unexpected inputs. The attack injection methodology mimics the fault injection methodology but may be particularly useful as a vulnerability testing technique since sophisticated cyber-security attacks may be injected to automatically identify security vulnerabilities in the system.

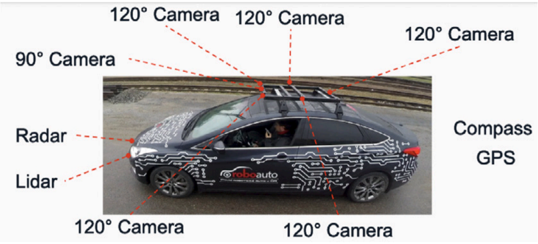


Fig. 5. Latest Roboauto model based on Hyundai i40.

The cost and effort of fault- and attack injection may be decreased by reducing the fault and attack space through pre-injection and post-injection (e.g. predictive) analyses. Pre-injection analysis may also be useful to derive effective attack injection sequences, e.g. to automatize penetration testing.

In VALU3S, we plan to investigate both analytical verification methods (e.g., formal methods) as well as machine learning methods supporting pre-injection analyses.

5. VALU3S use cases

In the VALU3S project, 13 use cases are considered and are described in the following, spanning all of the six domains covered by the project.

(1) ***Intelligent Traffic Surveillance.*** Unicam is a state-of-the-art and field-proven platform for creation of multifunctional and scalable intelligent vision-based and signal processing solutions. The platform has been used by CAMEA in two key areas: intelligent transportation systems and industrial inspection systems. All key technologies used for creating the innovative products are continuously developed by Camera. While OEM components are available for integration into current systems, fully featured systems are also being provided. The most typical examples of applications based on Unicam platform are Spot Speed Enforcement, Section Speed Enforcement, Travel Time, Red Light Enforcement, or Weigh-in-Motion system. The Unicam systems (e.g. Unicam VELOCITY — section speed measurement) are composed of a combination of a local processing on-site (LP detection and OCR) with all the infrastructure around (video cameras, IR flashes, PC, networking, etc.), and background processing running on the server side. Currently, on the sites, Unicam systems are updated with CAMEA's smart cameras with the ability of running licence plate video detection algorithms. Detection results are then sent to a server and processed in the meaning of the matching corresponding detection and calculating average speed. At any time, we have to prove the source of the data and time of the capture. We also have to ensure that the data cannot be counterfeited at any time. Thus, we aim at implementing data signing mechanisms with possible encryption directly in the smart camera. During the VALUE3S project, CAMEA is planning to investigate smart and mostly wireless sensors (cameras, radars, etc.) in terms of testing and verification of its reliability and security [61].

(2) ***Car Teleoperation.*** Roboauto initiative started in 2007 with a small model of a remote-controlled car, which was over the years improved and grew into the medium model. These models were

mainly participating in country robotic car competitions with the goal to get from point A to point B in a decent time without a defect or accident. The current model used by Roboauto is a real car – a Hyundai i40 (see Fig. 5) – with drive by wire support. The car has six cameras installed on the roof. In the front part, radar and lidar are installed to monitor surrounding traffic-related objects and possible obstacles on the road. The car also has a built-in compass and GPS location tracker. The computer located in the car trunk is processing the data from the sensors. It is connected with cameras through the GMSL bus, the rest of the sensors send data via CAN bus. The driving is currently done by means of remote control from the lab, which controls the car through the steering wheel and pedals. The module is connected to the LTE network, and the commands are then delivered to the car driving module. Roboauto must ensure the car is safe also in these cases: one of the cameras, radar or lidar, GPS or compass malfunctions, data mismatch between sensors (e.g. caused by delay), a delay in sensor data, a delay in remote control towards the car, decreased throughput of LTE network, line detection fails, and object detection malfunctions. In the VALU3S project, the focus is on safety in presence of decreased throughput of LTE network, and latency of the LTE network while performing teleoperation of the car.

(3) ***Radar system for ADAS.*** NXP provides radar ICs for ADAS functionality to the open market. With the development of new generation of radar ICs, enabling more autonomous driving functionalities, also the complexity of V&V rises. To tackle the increase of V&V complexity, higher levels of automation in the V&V are needed that allow higher coverage with more measurements while increasing testing speeds. Hence, NXP needs to develop a system that allows quicker validation while increasing test coverage. Such a system is a radar system test bench which is placed in a lab, and consists of at least a radar module in an anechoic chamber with various movable target simulators as well as a computer control for running the tests. Based on the system use cases, tests will be executed automatically.

(4) ***Human–Robot-Interaction in Semi-Automated Assembly Processes.*** The use case takes place on the shop floor level, and focuses on real-time object tracking and detection in industrial IoT environments. It is based on a wearable motion tracking sensing system combined with a low-energy single-board computer for data pre-processing, sensor fusion and wireless transmission. The described system can be considered as the means for a wider spectrum of sophisticated security, safety and context-oriented applications in IoT environments, such as collision avoidance [98,99]. The idea is to set up a real-time data stream processing pipeline to record external and internal sensor data of the HRI system. The aim of the use case scenario is to recognize and detect failures in the data stream which might lead to a malfunction of the collaborative robot and an injury of the human worker. This will form the basis to extract single data segments from the stream, and eventually to recognize faults within the data patterns. These sequential patterns will be labelled and stored in the cloud, while at the same time representing the main input for conducting machine learning techniques (classification or regression), typically Neural Networks or Support Vector Machines.

(5) ***Aircraft engine controller.*** To ensure that VALU3S technology is applicable to complex aircraft evaluation cases, United Technologies Research Centre Ireland (UTRCI: Part of Collins Aerospace) proposes a use case that will cover automated fault and attack injection, specifically to control the aircraft engine (Fig. 6). The engine use case will start by developing models of conventional main engines using existing state-of-the-art tools for modelling engine cycles, airflow, fuel dynamics and air compression. At the same time, the engine controller, a vital part of the engine both for its safety and fuel efficiency, will follow multiple design-cycles phases, based on the different control approaches and requirements of the use-cases. To this end, the VALU3S platform will be challenged to verify the different control approaches for its adjacent engine models, depicting pros and cons of the verification approach selected. The objectives of the use case are to evaluate the VALU3S technologies in an industrial setting for the independent aircraft components controlling the engine subsystems, combining a multi-domain analysis including fault and attack injection on the constituent co-models. The first activity of the use-case will be to develop an engine control module for a proof of concept engine plant system model, evaluating its realizability at software or hardware level. In parallel, a second activity will be to evaluate existing physical modelling tools used in current engine design phase, and investigate the interaction between cyber-models.

The engine to be studied will be a representative model of a high-bypass turbofan type used in commercial transportation, a typical instance of which is the so-called dual spool configuration, consisting of a fan, low and high speed compressors, as well as low and high speed turbines. The high-bypass characterization is derived by the fact that the majority of the air flow bypasses the core path (compressors and turbines) and only goes through the fan; this is in contrast to military aircraft, which are typically low-bypass for reasons of fuel efficiency at high speeds. In all modern turbofan engines there is a so called FADEC system (Full Authority Digital Engine Control), which monitors and controls everything about the engine, including thrust control, fuel control, power management, health monitoring of the engine, thrust reverser control, and so on. Due to this great amount of responsibility, a FADEC is typically designed with a high level of redundancy, in order to be fault tolerant, which typically leads to a quite complex implementation. What will be modelled for this use case is an appropriate abstraction of a FADEC with the ability to (a) respond fast/smoothly to pilot input, (b) maintain engine operation within acceptable limits (e.g. max fan/compressor speed, max turbine temperature, etc.), and (c) maintain steady state safe engine operation under no input change.

Finally, the verification activities for the aerospace use-case will also focus on the soundness and robustness of the approach, in order to achieve the maximum certification credit for the models developed, that will comply to aerospace regulations for software certification according to DO178C standard. In this context, safety and performance of the engine-controller pair will be evaluated under various types of faults (e.g. sensor faults, engine mechanical failures, abrupt changes in operating environment, etc.) in different flight phases (e.g. taxi or take-off).

(6) ***Agriculture robot.*** Energreen Company produces four multi utility and multi-tool tele-operated machines for Agriculture and Forestry called Agri-bot, transformed in autonomous robotic machines by E.S.T.E. The machine is a diesel engine powered multi-tool robot with two hydrostatic transmissions each controlling one track, both electronically controlled (by wire). The front tool is controlled by an Electronic Control Unit (ECU), and all the ECUs are connected through a SAE J 1939 CAN network. The robot can be a target of faults and attacks in different design and system aspects related to CAN networks, radio link for remote teleoperation, GPS, etc. The goal is to detect and identify such intrusions using both standardized existing approaches, such as [67,100], and their extension taking into account AI modelling techniques, such as [101].

(7) ***Human–Robot Collaboration in a disassembly process with workers with disabilities.*** Currently, the EU Machinery Directive (U.S. OSHA (29 CFR 1910)) and other regulations oblige machine manufacturers to install safety measures to protect operators and other employees from danger. In collaborative robotics,

the standard dictates the need to define four characteristics for a robot to be collaborative: (i) design the collaborative workspace; (ii) definition of the collaborative operation: minimum robot-operator separation, maximum speed, static and dynamic limits, ergonomics; (iii) methods for collaborative work: safety controlled stop, manual guidance, distance and speed control, etc.; and (iv) definition of the difference between collaborative/non-collaborative. The aim of the Fundación Aspace Navarra para el Empleo (FANE) organisation is to satisfy the labour needs of disabled people in order to make easier their integration in the common labour market (see e.g. [102]). The VALU3S technology can facilitate the thorough V&V activities that will be required by regulators for this type of technology by providing a validated platform for the systematic testing of complex software systems. The objective of this use case is to use the VALU3S in a collaborative robotic application;

(8) ***Neuromuscular Transmission for muscle relaxation measurements.*** This use case corresponds to a very innovative device for Neuromuscular Transmission (NMT) for muscle relaxation measurements. This device is aimed at simplifying the protocol to be followed by the Anaesthetists to monitor, in the operating room, the level of "Muscle Relaxation", i.e the deliberate paralysis of the totality of skeletal muscles of a patient under general anaesthesia. In VALU3S, we want to turn this device into an automated system that will be able to control the infusion pumps in order to keep the patient at a desired level of relaxation. This device uses a modified blood pressure cuff with stimulation electrodes to perform monitoring. The device has been a great success and highly appreciated by anaesthesiologists for its extreme simplicity of use, and has been certified for Europe and Japan. The 510 (k) process has been completed with the FDA, while China's regulation is in progress;

(9) ***Autonomous train operations.*** CAF Signalling has been working in Computer Vision (CV) & Artificial Intelligence (AI) based railway signal detector/identifier techniques. After several data recorded in the field (real railway journeys), CAF Signalling trains different object detectors/identifiers. Light signals (green, red, orange), static speed restrictions panels, platform stopping point signals or platform proximity signals have been labelled in different video databases in order to train these custom models. Although, the resulting models show accurate performances in nominal scenarios, they must be tested in higher variety of situations, extreme conditions and hazard situations in order to consider them really validated and certificated. However, diverse and complete database creation is expensive task in terms of time and budget. Moreover, it could be almost unaffordable task due to hazard situation only happens once in a long time or never. It is mandatory that well validated and verified system has been tested using databases containing different videos/clips representing all kind of (a) visibility conditions (meteorological, daylight or occlusions issues), (b) situations and behaviours of the static/dynamic object that are present in railway environment (e.g., pedestrian or vehicles) or (c) hazard combination of them. The global aims of this use case, is to set a semi-automatic V&V method, based on virtually generated scenarios to test the algorithm and AI model's robustness facing reduced visibility conditions. They will test over same railway journey but under different meteorological, daylight or partial occlusion conditions.

Currently, ongoing research is focused on; (a) V&V framework requirements and scenario definition/design, (b) visual scenario database generation changing weather, light and occlusion conditions using Train Simulator [103] video game scenarios, (c) metrics definition to measure the accuracy of tested CV&IA-enhanced application and (d) semi-automatic V&V framework prototype generation containing manually labelled ground truth (only first video as template) and automatic test and result analysis (see Fig. 7).

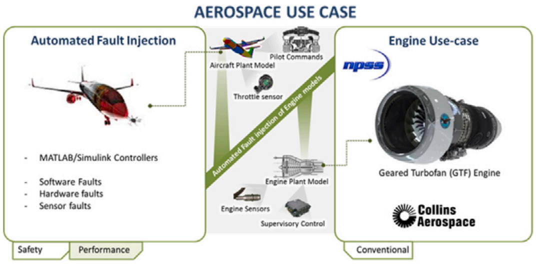


Fig. 6. UTRCI-Collins Aerospace use-case for automated fault-injection of engine models at simulation level.

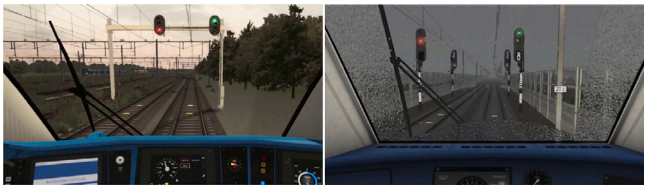


Fig. 7. Virtual environment which simulates a scenario under (a) sunny meteorological conditions and (b) rainy and foggy journey's meteorological conditions.

(10) ***Safe function out-of-context.*** This use case corresponds to safety-critical systems subjugated to various safety standards in the railway domain. In the railway domain, the typical error response time is 100 ms, and a typical scenario is a fault-detection of the motor control in the application. In this use case, we plan to implement a safety function (e.g. a safety stop) on two different platforms, and then move the safety function from one execution environment to another, and mimic the certification process. This way, we are able to validate if the methods and tools developed in the course of the VALU3S project support (i) a simplified (re-)certification process, (ii) reduce the cost and time for work on functional safety, and (iii) increases the system availability.

(11) ***Automated robot inspection cell for quality control of automotive body-in-white.*** The goal of this use case is to provide a better fault-tolerant production line to achieve better quality control for automotive body-in-white. Quality control has been carried out by means of the camera system positioned on the cartesian robot located on both sides of the vehicle body (i.e bus). The data obtained from the CAD data of the large-bodied vehicle is compared with the actual data obtained from the camera system by means of the synthetic data obtained from the developed data, and the item presence-absence check and critical measurement controls acquired from sensors and actuators, as shown in Fig. 8. To ensure that VALU3S technology is applicable to the robot inspection cell for quality control, in this use case, we will cover an automated fault and attack injection (see e.g. [19,68] and references therein for details), specifically for controlling the entire industrial automated line. The use case will be evaluated in the context of VALU3S considering security and safety, e.g. demonstrating results from simulations and the role of VALU3S in decision making, assessing full inspection processes in terms of task completion rate, duration and safety metric, considering time required to detect and overcome faults and attacks, and anomaly detection at component and system level by utilizing ML techniques.

(12) ***Total Knee Arthroplasty navigation system.*** Total Knee Arthroplasty (TKA) is a surgical procedure to resurface a knee damaged

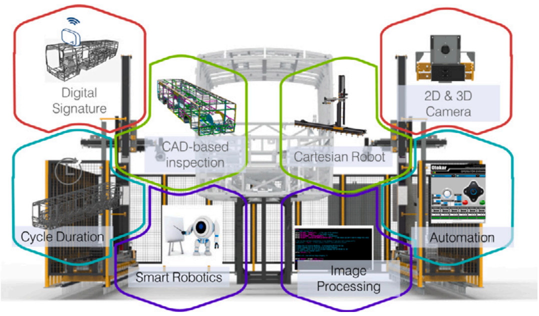


Fig. 8. The components of body-in-white inspection systems for world-selling OTOKAR buses.

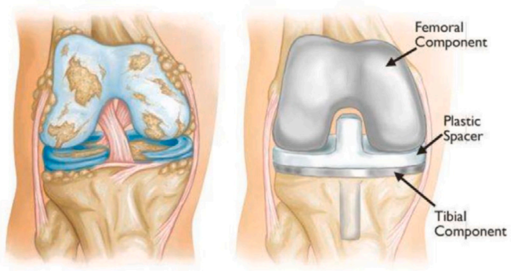


Fig. 9. (Left) pre-operative knee with severe arthritis; (right) post-operative knee with the implant.

by arthritis. Metal and plastic parts are used to cap the ends of the bones that form the knee joint (see Fig. 9). P3D is developing a new navigation system that leverages AI to minimize the impact of markers attachments to the patient. Instead, video from a cell-phone camera is used to automatically segment the bone regions of the image and match the reconstructed 3D surfaces to the pre-operative CT-scan or MRI of the patient. This new registration process uses Machine Learning computer vision techniques to learn the anatomy of the patient and recover the structure needed to guide the surgeon throughout the procedure. V&V activities in medical devices that contain AI softwares pose an added challenge for the manufacturer, and regulators are currently discussing strategies to ensure safety of medical devices that use such non-deterministic software modules. Upon entry in the market of an AI-based medical device, its performance is likely to be improved. Such modification could potentially require a re-submission of the medical device for the competent authorities for re-certification of the device, even if the intended use would remain the same. The VALU3S technology can facilitate and automate the thorough V&V activities that will be required by regulators for this type of technology by providing a validated platform for the systematic testing of complex software systems;

(13) ***Industrial Drives for Motion Control.*** The industrial drives for motion control use case focuses on a generic commercial motion control platform solution for permanent magnetic synchronous motors. The available system fo this case study was already designed in SESAMO & AQUAS ECSEL projects to comply to Safety Standard IEC 61508 and IEC 62443 from the security perspective. As a basis for VALU3S, one FPGA based hardware prototype along with a virtual prototype is available. VALU3S perfectly complements the previous work with respect to the focus on V&V. Especially the change towards the new processor architecture causes significant verification efforts of safety and security features where effective fault and attack injection can bring high value.

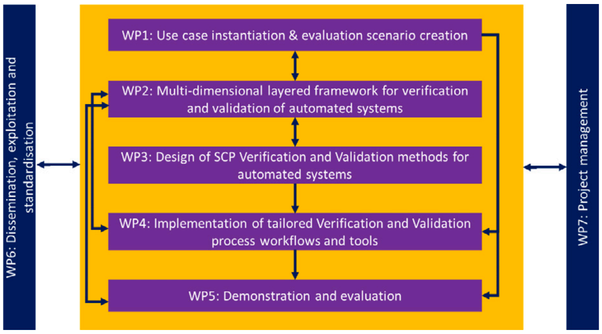

WP1: Use case instantiation & evaluation scenario creation
WP2: Multi-dimensional layered framework for verification and validation of automated systems
WP3: Design of SCP Verification and Validation methods for automated systems
WP4: Implementation of tailored Verification and Validation process workflows and tools
WP5: Demonstration and evaluation
WP6: Dissemination, exploitation and standardisation
WP7: Project management

Fig. 10. Connection between different WPs in VALU3S.

6. Implementation

6.1. Work packages

The work plan consists of 7 work packages, summarized in Fig. 10. A description of technical WPs contribution follows.

- ***WP1*** The main objective of the first work package in VALU3S is to gain insight into the evaluation scenarios for the various VALU3S use cases. For that, the VALU3S use cases and evaluation scenarios will be detailed out. These scenarios are a high-level classification of the underlying test requirements, which are grouped depending on their type such as functional, performance, safety, cyber-security and privacy, and will create VALU3S's repository of evaluation scenarios. The second objective in WP1 consists in producing the detailed descriptions of the evaluation scenarios and the derivation of respective test requirements. These requirements are the basis against which the systems will be verified during design and validated after implementation. With the insight gained addressing the first two objectives, the final objective of WP1 is to take the repository of evaluation scenarios and use cases across different domains. WP1 executes the first step of the methodology;
- ***WP2*** The main objective of this work package is to create a multi-dimensional layered framework for V&V of automated systems with respect to SCP requirements. The framework will be represented as a web-based repository where all elements of the framework will be stored. The repository is planned to be updated throughout the course of the project to take into account all the outputs provided by WP3–WP5;
- ***WP3*** The aim of this work package is to create the VALU3S reference set of methods to be used for the V&V of automated systems. To do so, an analysis of the commonly-used as well as state-of-the-art experimental and analytical V&V methods useful for evaluation of SCP requirements will be followed by identifying gaps and addressing those gaps with new and improved V&V methods. WP3 executes the second step of the methodology;
- ***WP4*** The aim of this work package is to design and implement a set of process workflows with tools for continuous simulated verification and validation of software systems' architectural design and implementation. The produced outcome will result in reducing the time and effort needed in V&V of automated systems. To this aim, the process is structured around (i) coupling between different V&V methods, (ii) identifying similarities between different environments, and (iii) optimization of already identified methods and development/improvement of tools for specific workflows. WP4 executes the third step of the methodology;
- ***WP5*** The goal of this work package is to integrate and evaluate the process workflows and tools designed and developed in WP4 in demonstrations. The demonstrators are built taking

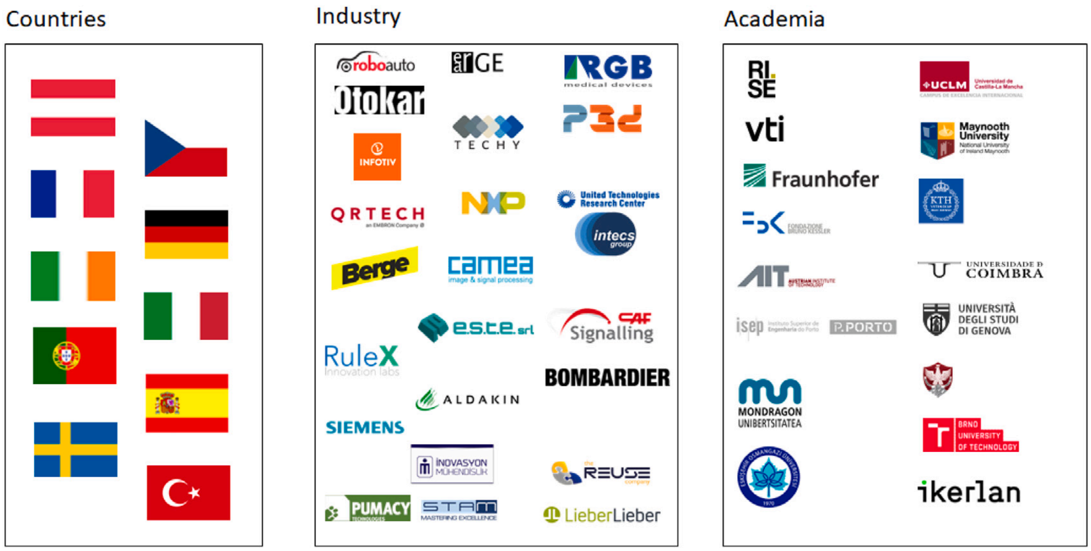


Fig. 11. VALU3S consortium.

into account the use cases and reference test scenarios identified in WP1. Demonstrations will cover different areas performing tests in the field evaluating V&V of solutions provided by use cases, evaluation of models of components linked with specific use cases in simulators, and developing test benches for evaluation of the V&V solution incorporating improved or newly designed methods. WP5 executes the fourth and final step of the methodology.

Finally, ***WP6*** will cover the dissemination, exploitation, and standardization actions to guarantee the impact of the results obtained in VALU3S, while ***WP7*** will deal with the overall management and coordination of the project.

6.2. Consortium as a whole

There are 16 academic partners (6 research institutes and 10 universities), and 25 industrial partners contributing to the project (see Fig. 11). The countries represented in the project are Austria (3 partners), Czech Republic (3 partners), France (1 partner), Germany (3 partners), Ireland (2 partners), Italy (7 partners), Portugal (3 partners), Spain (7 partners), Sweden (7 partners), and Turkey (5 partners).

7. Current status

7.1. WP1: Use case instantiation & evaluation scenario creation

The former studies in WP1 are focused on achieving insight into 13 use cases under 6 target domains (Aerospace, Agriculture, Automotive, Healthcare, Industrial Robotics/Automation, Railway). Firstly, definition and description of the use cases are completed in their target domain. Secondly, evaluation scenarios are identified for each use case. These scenarios are a result of interviews with stakeholders within the domains, the vast knowledge of the project partners on their domains of expertise and a close cooperation between partners in the VALU3S project i.e., UC providers and the V&V technology providers. All use cases have been mapped out and described with a total of 57 evaluation scenarios. This evaluation scenario repository is used as a high-level classification of the underlying 239 test requirements. Then, the test requirements and evaluation scenarios are used to design the test cases, 192 of which have been identified. Note that, the evaluation scenarios represent “What” needs to be evaluated, while the test cases describe “How” to test, and requirements will form the basis against which the systems will be verified during design and validated after implementation. The current studies in WP1 are focused on commonality evaluation of the use cases and test cases. Commonality analyses of the evaluation scenarios, the SCP requirements and test cases within the six target domains of the project are realized. The results show that Automotive and Industrial automation domains have more common points in terms of evaluation scenarios, SCP requirements and test cases with other domains. In this way, the automated systems in these domains will have the opportunity to use the same test case from component level to system level. At the same time, the identified test cases are being detailed and mapped to the dimensions/layers of the framework as defined by the work carried out so far in WP2.

7.2. WP2: Multi-dimensional framework design

The main objective of WP2 is to define a clear structure around the components and elements needed to conduct V&V processes through identification and classification of evaluation methods, tools, environments and concepts that are required to verify and validate automated systems with respect to SCP requirements. To this end a multi-dimensional framework has been designed for the third milestone of the project. The multi-dimensional framework design is the conceptual foundation of a Web repository to store the V&V information created by each of the Use Cases and tasks of VALU3S project. The Web repository will be populated with the test cases and requirements specification detailed in WP1, V&V methods in WP3, V&V tools identified and developed in WP4 and the evaluation results of the V&V process in WP5. The repository will store also outputs of WP1 and WP3–WP5 such as V&V methods, processes and tools.

The main aim of the framework is to allow storage of the V&V information in a uniform and homogeneous way, to facilitate exchange and retrieval of information. The framework specifies what data related with each V&V activity must be collected and defines the data format. This is done through designing and detailing a methodological framework, enabling the decomposition of elements and components required to conduct system V&V. Through a structured classification of the components required for the V&V of automated system the framework provides practitioners with detailed information about all components involved in the V&V process. That information facilitates the V&V process through identification of state-of-the-art V&V methods, tools and processes used in different domains, as well as the application of those methods to Use Cases. The framework is therefore a key instrument to achieve the main objective of the project, which is the design and development of V&V methods and tools that shorten time and lower cost of V&V processes.

To define and establish the way in which the framework is planned to be used, we have defined the framework's stakeholders. The potential users of the Web repository are divided in two main groups: (1) VALU3S project members and (2) community members. Community members are understood to be all those users who are not involved in the VALU3S project, but who are active in the domain of V&V of automated systems. The objective of defining the community stakeholder is to offer a public access to the VALU3S Web repository once the VALU3S project is finished. VALU3S framework include 8 different stakeholders types:

(1) V&V tool vendor;
(2) V&V researcher;
(3) Use Case provider;
(4) SW and HW developer;
(5) System designer;
(6) Test engineer;
(7) QA (Quality Assurance) engineer/project manager;
(8) QA manager.

The objective of each stakeholder differs with respect to their needs in the different activities of V&V. In order to identify the needs that the framework must cover for the different users, several user stories have been defined per stakeholder. These user stories define the functionalities to be implemented in the VALU3S Web repository and will be used in the validation process of its implementation. There are 4 main types of user stories related with V&V activities:

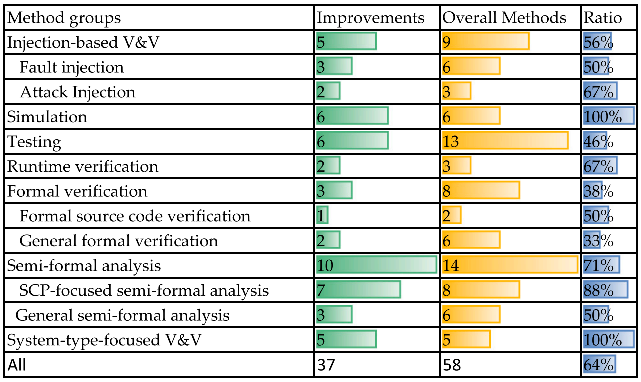
(1) Characterize V&V method,
(2) Characterize V&V tool,
(3) Search and compare V&V methods,
(4) Search and Compare V&V tools.

A total of 24 user stories have been specified in a UML use case diagram. In order to describe the design and structure of the V&V multi-dimensional framework, a UML class diagram has been created. The central element of the UML class diagram is the V&V Method or Technique that could be an evaluation method that is added to the framework. These methods are categorized using the dimensions, by means of many-to-one and many-to-many relationships between the V&V Method/Technique entity and the various dimensions. The framework currently has 8 dimensions that are planned to be further detailed and extended in the course of the project.

Taking as input the VALU3S framework, the Web repository is intended to serve as a searchable catalogue of V&V methods applicable to specific domains and application scenarios. The project partners have the goal of populating it with the V&V information generated throughout the project. For the implementation of the Web repository, the Plone [104] content management system has been selected and the team has completed the first phase of tailoring it to the needs specified in the requirements. Development shall continue to support the requirements elicited throughout the project. Namely, a user shall be able to characterize a V&V method or tool, by relating those with the framework's dimensions, and shall be able to search and compare existing V&V methods or tools. To this end, the objective is to create a transformation from the data model to the XML definitions accepted by the Plone CMS, based on the designed framework.

7.3. WP3: Design of SCP V&V methods for automated systems

Work Package 3 is focused on the development of new V&V methods that can fill the current gaps. The first task was the study of the State of the Art of the existing V&V methods to populate a repository which can be used as a reference for the whole project. These methods are currently applied or could be applied in the project use cases and can improve how SCP requirements are addressed, ensured, and confirmed. Fifty-eight methods are described by presenting their name, purpose, description, tool support, strengths and weaknesses. The methods have been divided in seven categories: *Injection-Bases V&V*, *Simulation*, *Testing*, *Run-time Verification*, *Formal Verification*, *Semi-Formal Analysis*, and *System-Type-Focused V&V*. All the methods have been mapped into the multi-dimensional framework defined in WP2: they cover a wide range of SCP evaluation needs of automated systems, from source code analysis and behaviour assessment to earlier needs in a system's life-cycle such as safety analysis during design. The methods cover both formal and non-formal V&V and exploit different means such as models and ontologies. The subsequent step, which ran from months 8 to 12 of the project was the identification of gaps and limitations of the existing methods. This is done both from a method perspective (i.e. identifying limitations in the method itself) and from a use case point of view (i.e. finding gaps that prevent the application of a method in a specific scenario). Overall, 400 gaps in the groups: Functionality, Accuracy, Scalability and Computational, Deployment, Learning Curve, Automation, Reference environment, Cost, and Standards, were found. The identification of gaps allows to address them in the last task of the WP: the definition of new V&V approaches. These new techniques may consist both in completely new methods, in improvement of existing methods or, even, in *married* methods that put together two different approaches to overcome their limitations. At the time of writing, for 37 methods, concrete improvements were sketched and work on several of them has started, summarized in Fig. 12. Four new combinations of methods have been sketched as well. Together, they address 145 of the gaps. In addition to developing the already listed methods, further gaps and improvements might be identified and addressed while detailing the use cases and developing the demonstrators for the use cases in the second project year.



Method groups	Improvements	Overall Methods	Ratio
Injection-based V&V	5	9	56%
Fault injection	3	6	50%
Attack Injection	2	3	67%
Simulation	6	6	100%
Testing	6	13	46%
Runtime verification	2	3	67%
Formal verification	3	8	38%
Formal source code verification	1	2	50%
General formal verification	2	6	33%
Semi-formal analysis	10	14	71%
SCP-focused semi-formal analysis	7	8	88%
General semi-formal analysis	3	6	50%
System-type-focused V&V	5	5	100%
All	37	58	64%

Fig. 12. Distribution of improved methods.

7.4. WP4: Implementation of tailored V&V workflows and tools

Work package 4 aims at the design and implementation of process workflows with dedicated tool chains. It integrates V&V methods from work package 3 and enables the evaluation of the industrial use cases in WP5.

The first task 4.1 deals with the preparation of the workflow design for VALU3S solutions and their implementation as use-case-specific tool chains. Partners will be enabled and prepared to design and implement dedicated workflows for the use cases, V&V methods, and tools in the project.

Initial results from work package 1 on use case scenarios, test cases, and preselected tools, from work package 2 on the VALU3S framework, and from work package 3 on V&V methods, tools, and tool combinations is currently being analysed regarding requirements, assets, and constraints for the V&V workflow design. Special attention is paid to the available and planned V&V tools from the VALU3S partners to facilitate tool usage and integration and enable automated and practicable V&V workflows for the various use case scenarios in the project. Technical details on tool interfaces, exchange formats and execution environments, and legal questions regarding licencing is elicited.

Additionally, possible tool support for efficient and user-friendly workflow design modelling will be investigated, exploiting the expertise and solutions in the area of model-based software and systems engineering and tool interoperability of the VALU3S technology providers. The goal is to develop a generic V&V workflow design approach and modelling language that allow tool-supported and highly automated instantiation to specific industrial use cases and implementation as concrete tool chains. This approach will pave the way towards the efficient evaluation and optimization of V&V workflows and tool chains for specific SCP properties. The activity will be performed in close cooperation with work package 3 to support the systematic description, extension, and gap analysis of V&V methods.

7.5. WP5: Demonstrators and evaluation

Primary goal of work package 5 is to demonstrate the usefulness of the VALU3S framework with improved or newly created methods and tools developed in work packages 3 and 4. The demonstration will consist of several, so called, demonstrators selected from all use cases (specified in work package 1) to provide complete coverage of all domains, all layers and dimension of the V&V framework. Demonstrators are a joint work of experts from different fields of V&V led by 13 use case providers. One of the main parts of demonstration is an evaluation report which that documents how much the quality of a developed system increased and how much time and cost required for V&V processes can be reduced. To provide a credible evaluation, several metrics have been defined, focusing both on measuring safety, cyber-security, and privacy features, and on measuring the cost, effort, and quality of V&V process used in engineering processes in different use cases.

Verification and validation are complex processes combining different approaches and incorporating many different methods. These processes differ a lot depending on the type of system under test, priorities of system requirements, severity and criticality of developed features, and the amount of available resources (including but not limited to software tools for verification, their licences, and hardware testbeds). Comparing the improvement provided by the VALU3S project on all the demonstrators with their different V&V processes is not an easy task. There is no single metric which can simply measure, by a unified scale, the different approaches to V&V and their complex characteristics. In VALU3S, we have decided that at least two different points of view must be considered to get a sufficient overview of how well V&V performs:

(1) Evaluation of safety, cyber-security, and privacy
(2) Evaluation of V&V processes

Both evaluations can be supported by different metrics, i.e., the evaluation will target specific criteria. Moreover, one criterion targets a single aspect or a few of them and cannot express all the features of a complex V&V process. Combining different evaluation criteria while evaluating the demonstrator will bring more value and put more light to the status of V&V.

Currently, the initial plan for the demonstration has been prepared. The plan consists of 5 steps:

(1) Initial definition of demonstrators and specification of baselines.
(2) Specification of evaluation criteria and evaluation of the baselines.
(3) Implementation of demonstrators.
(4) Evaluation of the whole V&V framework.
(5) Final demonstration at the end of the VALU3S project.

The first two steps are partially done; 13 demonstrators have been identified from all the use cases, the baseline of each of the demonstrators identifies current status of the development, and 17 evaluation criteria for SCP and 13 evaluation criteria for V&V processes have been specified.

7.6. WP6: Dissemination, exploitation and standardization

The goal of this Work Package is to plan, define, and implement all the necessary activities focused on dissemination, training, exploitation, standardization, and communication that will guarantee the aimed impact of VALU3S' results. Thus, initial plans for these activities have been defined and their implementation has been set in place (details have been presented in the corresponding internal deliverables). The progress made so far in this work package comprises:

- **Dissemination and Training:** there were several actions pursued to establish the processes that guarantee that all published material respect the requirements of the project's Grant Agreement and Project Consortium Agreement, including that open access is ensured. To that end, both a detailed publication workflow and a database were defined to keep track of publications. In what concerns training activities, two surveys have been distributed to the consortium in order to obtain data to support organizing training sessions. Based on that collected data, the first training session of the project has been organized, totalling 11 presentations on distinct V&V methods (the videos are available in VALU3S' YouTube channel [105]).
- **Exploitation:** the main results are the development of an initial plan for exploitation that identifies the main operational results and the methodology that will be applied to achieve the objectives of the project, a short- and long-term market analysis including the examination of the different target markets that the results obtained within VALU3S may reach (according to the domain in which they have been developed and the type of organization that intends to exploit them). Also relevant was the definition of a set of KPIs which will allow to accurately monitor the progress of exploitation activities along the project.
- **Standardization:** the focus was given to standards and standardization related to the work in VALU3S. For that purpose, a survey was designed based on a list of initially identified standards with the objective of collecting further relevant standards and start the evaluation of relevant methods, tools and approaches related to the work planned for the project. The results of the survey are now being used to give feedback to tasks related to methods and framework development, e.g., to associate methods and tools with the relevant standards, and also to setup an initial set of methods and tools where partners and external stakeholders might be interested in for training purposes.
- **Communication:** the focus of the initial work done in the project was to define an initial plan to carry out a set of communication activities that can promote VALU3S project partners and outcomes towards a general audience, as well as pave the way to VALU3S platform commercialization engaging potential stakeholders and customers. This includes a set of relevant actions like implementing blog articles with high-level technical content, production of communication materials and, importantly, setting up and triggering the actions for the creation of liaisons with other related R&D projects in order to maximize the impact of dissemination and communication activities. Communication in the project's social media channels has also been a key activity that includes regular posts of partners profiles, announcement of new project publications, and also videos related to activities in the project.

7.7. WP7: Project management

The activities of this work package (WP) have started from the first day of the project and will continue till the end of the project. Multiple working groups and committees have been created within this WP, contributing to the smooth execution of the project. These groups include project's technical and steering committees and a cross-task group which is used as a platform to synchronize on the discussion points that go beyond the borders of a certain WP. Several coordination meetings have been scheduled and organized for each of the above-mentioned groups to follow-up on fulfilment of the project objectives as well as to mitigate any potential risks posed to the fulfilment of the objectives due. In addition to these meetings, multiple project consortium meetings have been scheduled and organized since the beginning of the project to mitigate the negative impact of the COVID-19 pandemics [106] that has resulted in lack of face-to-face project meetings. All the risks identified have been included in a risk register created for the project, which is the basis of the risk assessments adopted in the project.

The activities within this WP also resulted in the selection and structuring of the project collaboration tools as well as the submission of 8 deliverables, all contributing to the overall management of the project. Part of these deliverables are dedicated to planning of the upcoming project milestones as well as analyses of the previous milestones. The project has 8 milestones and we have already validated the results obtained in the first four milestones of the project. An important activity within WP7 has been the creation and maintaining of the project handbook. In the handbook, we gather essential and practical information about financial, administrative and managerial procedures used in the project. This includes:

- **Project management** and the roles of different people and committees involved in the management of the project.
- **Internal communication** including the preferred online meeting platforms, e-mail culture, and social media channels.
- **Technical reporting** including the procedures around how and when the technical progress reports need to be provided as well as when the project deliverables need to undergo an internal review. The internal review process has been created in a way so that we deliver and submit project deliverables with high-quality.
- **Financial reporting** that includes the procedure details about annual financial reports to the commission as well as internal quarterly reports.
- **Quality management** where the validation and analysis of the project milestones are discussed and detailed. This is also where the project risk management process is detailed.

8. VALU3S impact and alignment with EU goals

As aligned with the EU goals formulated within the concept of Digital Single Economy [107], VALU3S fosters a horizontal solution stack supporting the effective exploitation of smart systems in all priority areas of ECS SRA 2020 [108]. Thus, VALU3S focuses on the V&V of smart systems in five key application areas mentioned in the ECS SRA, i.e. transport and smart mobility, health and wellbeing, energy, digital industry and digital life, which will play a crucial role in improving EU's economic competitiveness.

VALU3S impacts are not limited to the direct technology and economic factors but the project also has indirect impacts on political, legal, environmental and social improvements. Direct impacts in technology domain rely on scientific improvements in new technological paradigms like the advent of AI and data analytics, advances in computing with new hardware and software-based V&V techniques, increased connectivity and heterogeneity with IoT-driven cyber–physical systems, and comprehensive SCP mechanisms. The developments in these areas will significantly influence the economy by creating new expertise areas relying on the application of advanced V&V techniques. The duties of security officers, system integrators, auditors, system engineers, etc. can be revised according to VALU3S outputs and recommendations. VALU3S may create new business opportunities as the results of the project can be spread to other countries. Moreover, project results can be used directly in top sectors where EU leads with other G20 countries, such as automotive, rail, aerospace, health and pharmacy, agriculture and food, production, etc. accelerating new business and collaboration opportunities and reduce the investment and maintenance costs.

The indirect impacts of VALU3S have a wide spectrum in terms of EU policy development, environmental protection and social factors. VALU3S has a very strong compliance and contribution strategy regarding standards. The project achievements will help decision-makers or rule-makers to improve the safety, security (GDPR) and trade regulations and policies. VALU3S will also have a significant effect on reducing the carbon footprint and reaching the zero-carbon goals by applying effective V&V mechanisms to reduce accidents that may cause pollution, shorten production times and increase the yield, and to apply AI-enabled waste management and resource planning and realize energy-saving techniques. VALU3S will finally impact the social life as the worker safety will be improved, protection of personal data will be enhanced and labour saving will be provided, all of which will upgrade the working conditions.

9. Conclusions

This paper presents the VALU3S ECSEL JU project. It discusses the challenges arising from the V&V safety, cyber-security and privacy (SCP) of automated systems. The project goal is to design, implement and evaluate state-of-the-art of V&V methods and tools to reduce the time and cost needed to verify and validate SCP requirements of automated systems. The project builds upon the knowledge that partners gained in current or former EU projects and will demonstrate the newly conceived approaches to co-engineering across use cases spanning Automotive, Agriculture, Railway, Healthcare, Aerospace, and Industrial robotics. It is worth noting some ECSEL projects that have provided background and/or reusable results taken into account in VALU3S: MegaM@rt2 [109], AQUAS [110] and AFarCloud [111].

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

Special thanks to all VALU3S consortium members that have worked on the VALU3S proposal on which this paper is based on, especially to Behrooz Sangchoolie, the proposal coordinator. The VALU3S project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No. 876852. The JU receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Czech Republic, Germany, Ireland, Italy, Portugal, Spain, Sweden, Turkey. The views expressed in this document are the sole responsibility of the authors and do not necessarily reflect the views or position of the European Commission. The authors, the VALU3S Consortium, and the ECSEL JU are not responsible for the use which might be made of the information contained in here.

References

[1] http://www.rgb-medical.com/en/special-product/tof-cuff-nmt-monitor.

[2] Y.Z. Lun, A. D'Innocenzo, F. Smarra, I. Malavolta, M.D. Di Benedetto, State of the art of cyber-physical systems security: An automatic control perspective, J. Syst. Softw. 149 (2019) 174–216.

[3] A. D'Innocenzo, M.D. Di Benedetto, F. Smarra, Fault detection and isolation of malicious nodes in MIMO multi-hop control networks, in: 52nd IEEE Conference on Decision and Control, IEEE, 2013, pp. 5276–5281.

[4] ECS-SRA, 2018, https://www.smart-systems-integration.org/publication/ecs-sra-2018.

[5] VALU3S Project - https://valu3s.eu/.

[6] Trend Micro Research, Security Threats and Risks in Smart Factories, https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/security-threats-and-risks-in-smart-factories.

[7] Strategic Research Agenda - https://www.smart-systems-integration.org/publication/ecs-sra-2018.

[8] F. Smarra, G.D. Di Girolamo, V. De Iuliis, A. Jain, R. Mangharam, A. D'Innocenzo, Data-driven switching modeling for MPC using regression trees and random forests, Nonlinear Anal. Hybrid Syst. 36 (2020) 100882.

[9] M. Mongelli, S. Scanzio, A neural approach to synchronization in wireless networks with heterogeneous sources of noise, Ad Hoc Netw. 49 (2016) 1–16.

[10] B. Sangchoolie, P. Folkesson, J. Vinter, A study of the interplay between safety and security using model-implemented fault injection, in: 2018 14th European Dependable Computing Conference, EDCC, IEEE, 2018, pp. 41–48.

[11] S. Chatterjee, What are the benefits of using artificial intelligence in testing.

[12] P. Pop, D. Scholle, I. Sljivo, Safe cooperating cyber-physical systems using wireless communication, Microprocess. Microsyst. 53 (2017) 42–50.

[13] E. Per, E. Strandberg, W. Enoiu, D. Afzal, R. Sundmark, Feldt, Information flow in software testing – An interview study with embedded software engineering practitioners, J. IEEE Access (Apr 2019).

[14] R. Beard, Failure accomodation in linear systems through self-reorganization, Mass. Inst. Technol. (1971).

[15] H. Jones, Failure detection in linear systems, (Ph.D. Dissertation), Mass. Inst. of Technol, Cambridge, MA, USA, 1973.

[16] M.-A. Massoumnia, G. Verghese, A. Willsky, Failure detection and identification, IEEE Trans. Automat. Control 34 (3) (March 1989) 316–321.

[17] C. De Persis, A. Isidori, A geometric approach to nonlinear fault detection and isolation, IEEE Trans. Automat. Control 46 (6) (2001) 853–865, June 2001.

[18] A. Innocenzo, M. Di Benedetto, E. Serra, Fault tolerant control of multi-hop control networks, IEEE Trans. Automat. Control 58 (6) (2013) 1377–1389, June 2013.

[19] A. D'Innocenzo, F. Smarra, M.D. Di Benedetto, Resilient stabilization of multi-hop control networks subject to malicious attacks, Automatica 71 (2016) 1–9.

[20] F. Smarra, A. Jain, T. De Rubeis, D. Ambrosini, A. Innocenzo, R. Mangharam, Data-driven model predictive control using random forests for building energy optimization and climate control, Appl. Energy 226 (April 2018) 1252–1272.

[21] T. Kuhn, P. Antonino De Assis, M. Damm, A. Morgenstern, D. Schulz, C. Ziesche, T. Müller, Industrie 4.0 Virtual Automation Bus, in: IEEE/ACM 40th International Conference on Software Engineering: Companion ICSE-Companion, 2018.

[22] BaSyx, an open source platform for next generation automation, https://wiki.eclipse.org/BaSyx.

[23] E. Khalastchi, M. Kalech, On fault detection and diagnosis in robotic systems, ACM Comput. Surv. 51 (1) (2018) 9.

[24] S. Sridhar, A. Hahn, M. Govindarasu, Cyber-physical system security for the electric power grid, Proc. IEEE 100 (2012) 210–224.

[25] C.-C. Sun, A. Hahn, C.-C. Liu, Cyber security of a power grid: State-of-the-art, Int. J. Electr. Power Energy Syst. 99 (2018) 45–56.

[26] K. Huang, Assessing the physical impact of cyberattacks on industrial cyber-physical systems, IEEE Trans. Ind. Electron. 65 (2018) 8153–8162.

[27] Stuxnet and the Future of Cyber War-https://www.tandfonline.com/doi/abs/10.1080/00396338.2011.555586, 2011.

[28] S. Ashby, Emerging IT risks: Insights from german banking. The geneva papers on risk and insurance-issues and practice, 43, 80–207, 2018.

[29] S. Kumar, Evaluation of Ensemble Machine Learning Methods in Mobile Threat Detection, in: Proc. 12th Int. Conf. for Internet Technology and Secured Transactions ICITST, 2017.

[30] A. Joshi, S. Miller, M. Whalen, M. Heimdahl, A Proposal for Model-Based Safety Analysis, IEEE Computer Society, 2005.

[31] M. Bozzano, A. Villafiorita, Design and Safety Assessment of Critical Systems, CRC Press, Taylor and Francis, an Auerbach Book, 2010.

[32] M. Bozzano, A. Cimatti, J. Katoen, V. Nguyen, T. Noll, M. Roveri, Safety, dependability and performance analysis of extended AADL models, Comp. J. 54 (5) (2011) 754–777.

[33] ARP4761 guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment, 1996, December 1996.

[34] European Cooperation on Space Standardization - http://www.ecss.nl.

[35] B. Bittner, M. Bozzano, R. Cavada, A. Cimatti, M. Gario, A. Griggio, C. Mattarei, A. Micheli, G. Zampedri, The xSAP Safety Analysis Platform, in: Proceedings of TACAS, 2016.

[36] T.A. Henzinger, P. Ho, H. Wong-Toi, HYTECH: A Model checker for hybrid systems, STTT 1 (1–2) (1997) 110–122.

[37] G. Frehse, PHAVer: Algorithmic verification of hybrid systems past HyTech, STTT 10 (3) (2008) 263–279.

[38] G. Frehse, C.L. Guernic, A. Donzé, S. Cotton, R. Ray, O. Lebeltel, R. Ripado, A. Girard, T. Dang, O. Maler, SpaceEx: Scalable Verification of Hybrid Systems, in: CAV, 2011, pp. 379–395.

[39] S. Ratschan, Z. She, Safety verification of hybrid systems by constraint propagation-based abstraction refinement, ACM Trans. Embedded Comput. Syst. 6 (1) (2007).

[40] E. Asarin, T. Dang, O. Maler, The d/dt Tool for Verification of Hybrid Systems, in: CAV, 2002, pp. 365–370.

[41] X. Chen, E. Ábrahám, S. Sankaranarayanan, Flow*: An Analyzer for Non-linear Hybrid Systems, in: Computer Aided Verification - 25th International Conference, CAV 2013, Saint Petersburg, Russia, July 13-19, 2013. Proceedings, 2013, pp. 258–263.

[42] A. Platzer, J. Quesel, KeYmaera: A hybrid theorem prover for hybrid systems (system description), IJCAR (2008) 171–178.

[43] A. Cimatti, A. Griggio, S. Mover, S. Tonetta, in: C. Baier, C. Tinelli (Eds.), HyComp: An SMT-Based Model Checker for Hybrid Systems, TACAS, in: Lecture Notes in Computer Science, 9035, Springer, 2015, pp. 52–67, http://dx.doi.org/10.1007/978-3-662-46681-0_4.

[44] A. Tiwari, HybridSAL Relational Abstracter, in: CAV, 2012, pp. 725–731.

[45] J. Liu, N. Zhan, H. Zhao, Computing semi-algebraic invariants for polynomial dynamical systems, in: Proceedings of the 11th International Conference on Embedded Software, EMSOFT 2011, Part of the Seventh Embedded Systems Week, ESWeek 2011, Taipei, Taiwan, October 9-14, 2011, 2011, pp. 97–106, http://dx.doi.org/10.1145/2038642.2038659.

[46] S. Tonetta, Abstract model checking without computing the abstraction, in: FM 2009: Formal Methods, Second World Congress, Eindhoven, the Netherlands, November 2-6, 2009. Proceedings, 2009, pp. 89–105, http://dx.doi.org/10.1007/978-3-642-05089-3_7.

[47] S. Graham, P. Kessler, M. Mckusick, Gprof: A call graph execution profiler, in: Proc. of the 1982 SIGPLAN Symposium on Compiler Construction, 1982, pp. 82.

[48] Rapita Systems - https://www.rapitasystems.com/.

[49] G. Nelissen, A Novel Run Time Monitoring Architecture for Safe and Efficient Inline Monitoring, in: Proc. Ada-Europe International Conference on Reliable Software Technologies, 2015.

[50] J. Jahic, M. Jung, T. Kuhn, C. Kestel, N. Wehn, A Framework for Non-intrusive Trace-driven Simulation of Manycore Architectures with Dynamic Tracing Configuration, in: International Conference on Runtime Verification, Limassol, Cyprus, 2018.

[51] J. Jahić, T. Kuhn, M. Jung, N. Wehn, BOSMI: a framework for non-intrusive monitoring and testing of embedded multithreaded software on the logical level, 2018, Samos, Greece.

[52] L. Shannon, P. Chow, Using reconfigurability to achieve real-time profiling for hardware/software codesign, in: Proc. ACM/SIGDA 12th Int. Symp. Field Programmable Gate Arrays, Monterey, CA, 2004, pp. 190-199.

[53] J. Tong, M. Khalid, Profiling tools for FPGA-based embedded systems: Survey and quantitative comparison, J. Comput. 3 (6) (June 2008) 1–14, June 2008.

[54] P. Di Felice, M. Ianni, L. Pomante, A spatial extension of TinyDB for wireless sensor networks, in: 2008 IEEE Symposium on Computers and Communications, 2008, pp. 1076–1082.

[55] L. Pomante, C. Rinaldi, M. Santic, S. Tennina, Performance analysis of a lightweight RSSI-based localization algorithm for Wireless Sensor Networks, in: International Symposium on Signals, Circuits and Systems ISSCS2013, 2013, pp. 1–4.

[56] J. Yick, B. Mukherjee, D. null, Wireless sensor network survey, Comput. Netw. 52 (2008) 2292–2330.

[57] L. Berardinelli, A.D. Marco, S. Pace, L. Pomante, W. Tiberti, Energy consumption analysis and design of energy-aware WSN agents in fUML, in: G. Taentzer, F. Bordeleau (Eds.), Modelling Foundations and Applications - 11th European Conference, ECMFA@STAF 2015, L'Aquila, Italy, July 20-24, 2015. Proceedings, in: Lecture Notes in Computer Science, vol. 9153, Springer, 2015, pp. 1–17, http://dx.doi.org/10.1007/978-3-319-21151-0_1.

[58] N. Mohamed, J. Al-Jaroodi, Service-Oriented Middleware Approaches for Wireless Sensor Networks, in: Proc. 44th Hawaii International Conference on System Sciences, HICSS, Jan. 2011, pp. 1–9.

[59] E. Shi, A. Perrig, Designing secure sensor networks, Wirel. Commun. Mag. 11 (6) (Dec. 2004).

[60] D. Carman, P. Kruus, B. Matt, Constraints and Approaches for Distributed Sensor Network Security, Tech. Rep, 2000.

[61] L. Pomante, M. Pugliese, S. Marchesani, F. Santucci, WINSOME: A middleware platform for the provision of secure monitoring services over wireless sensor networks, in: 2013 9th International Wireless Communications and Mobile Computing Conference, IWCMC 2013, 2013, pp. 706–711.

[62] L. Freitas, K. Bispo, N. Rosa, P. Cunha, SM-Sens: Security middleware for Wireless Sensor Networks, in: Proceedings of the Information Infrastructure Symposium, 2009.

[63] R. Daidone, G. Dini, M. Tiloca, STaR: a Reconfigurable and Transparent middleware for WSNs security, in: Proceedings of the 2nd International Conference on Sensor Networks, SENSORNETS 2013, 2013.

[64] P. Chapin, C. Skalka, SpartanRPC: Secure WSN middleware for cooperating domains, in: Proceedings of the Seventh IEEE International Conference on Mobile Ad-Hoc and Sensor Systems, 2010.

[65] S. Marchesani, L. Pomante, M. Pugliese, F. Santucci, Definition and development of a topology-based cryptographic scheme for wireless sensor networks, in: M. Zuniga, G. Dini (Eds.), Sensor Systems and Software - 4th International ICST Conference, S-Cube 2013, Lucca, Italy, June 11-12, 2013, Revised Selected Papers, in: Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 122, Springer, 2013, pp. 47–64, http://dx.doi.org/10.1007/978-3-319-04166-7_4.

[66] W. Tiberti, F. Caruso, L. Pomante, M. Pugliese, M. Santic, F. Santucci, Development of an extended topology-based lightweight cryptographic scheme for IEEE 802.15.4 wireless sensor networks, Int. J. Distrib. Sens. Netw. (ISSN: 1550-1477) 16 (2020) URL https://doi.org/10.1177/1550147720951673.

[67] L. Corradetti, D. Gregori, S. Marchesani, L. Pomante, M. Santic, W. Tiberti, A renovated mobile agents middleware for WSN porting of Agilla to the TinyOS 2.x platform, in: 2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a Better Tomorrow, RTSI 2016, 2016.

[68] L. Bozzi, L. Giuseppe, L. Pomante, M. Pugliese, M. Santic, F. Santucci, W. Tiberti, TinyWids: A WPM-based intrusion detection system for TinyOS2.x/802.15.4 wireless sensor networks, in: ACM International Conference Proceeding Series, 2018, pp. 13–16.

[69] A. Causevic, Risk Assessment in Autonomous System of Systems-A Review, Vasteras, Sweden.

[70] T. Srivatanakul, J. Clark, F. Polack, Effective Security Requirements Analysis: HAZOP and Use Cases, Springer, Berlin Heidelberg, Berlin; Heidelberg, 2004.

[71] P. Feiler, J. Delange, C. null, Mellon Automated Fault Tree Analysis from AADL Models Software Engineering Institute 4500 5th Avenue, Pittsburgh.

[72] N. Leveson, N. Dulac, Safety and risk driven design in complex systems of systems, in: Proceedings of the 1st NASA/AIAA Space Exploration Conference, American Institute Of Aeronautics And Astronautics, Orlando, USA, 2005.

[73] J. Andrews, S. Dunnett, Event-tree analysis using binary decision diagrams, IEEE Trans. Reliab. (2000).

[74] P. Oliveira, M. Jung, A. Morgenstern, F. Fassnacht, T. Bauer, A. Bachorek, T. Kuhn, E. Nakagawa, Enabling Continuous Software Engineering for Embedded Systems Architectures with Virtual Prototypes, European Conference on Software Architecture, Madrid, 2018.

[75] P. Forbrig, BizDevOps and the Role of S-BPM, International Conference on Subject-Oriented Business Process Management, Linz, Austria, 2018.

[76] J. Justo, N. Araujo, A. Garcia, Software reuse and continuous software development: A systematic mapping study, IEEE Lat. Am. Trans. 16 (2018) 1539–1546.

[77] S. Uzunbayir, K. Kurtel, A Review of Source Code Management Tools for Continuous Software Development, International Conference on Computer Science and Engineering UBMK, Sarajevo, Bosnia and Herzegovina, 2018.

[78] P. O'hearn, Continuous Reasoning: Scaling the impact of formal methods, Symposium on Logic in Computer Science, Oxford, United Kingdom, 2018.

[79] M. Rodriguez, M. Piattini, C. Ebert, Software verification and validation technologies and tools, IEEE Softw. 36 (2019) 13–24.

[80] M. Shahin, M. Zahedi, M. Babar, L. Zhu, An empirical study of architecting for continuous delivery and deployment, empirical software engineering, 2018, 1–48.

[81] C. Carrillo, C. Rafael, S. Betz, B. Penzenstadler, T. Crick, S. Crouch, E. Nakagawa, C. Becker, C. Carrilloi, Software sustainability: Research and practice from a software architecture viewpoint, J. Syst. Softw. 138 (2018) 174–188.

[82] R. Larrucea, E. Fernandes, P. Acosta, X. Larrucea, A case analysis of enabling continuous software deployment through knowledge management, Int. J. Inf. Manage. 40 (2018) 186–189.

[83] M. Aramrattana, T. Larsson, J. Jansson, A. Nåbo, A simulation framework for cooperative intelligent transport systems testing and evaluation, Transp. Res. F (2019) 268–280.

[84] P. Lopez, M. Behrisch, L. Bieker-Walz, J. Erdmann, Y.-P. Flötteröd, R. Hilbrich, L. Lücken, J. Rummel, P. Wagner, E. Wießner, Microscopic Traffic Simulation using SUMO, in: The 21st IEEE International Conference on Intelligent Transportation Systems, Maui, HI, USA, 2018.

[85] C. Sommer, R. German, F. Dressler, Bidirectionally coupled network and road traffic simulation for improved IVC analysis, IEEE Trans. Mob. Comput. 10 (1) (2011) 3–15.

[86] I. Caterpillar, Cat minestar, 2016, http://www.cat.com, 2016-05-10.

[87] Hitachi, Hitachi to develop autonomous haulage system, 2016, 2016-05-10.

[88] Sandvik, Automine hauling, 2016, http://mining.sandvik.com, 2016-05-10.

[89] DesignatedDriver.ai, Blog About Teleoperation, Blog about teleoperation - https://designateddriver.ai/2019/01/why-teleoperation-of-autonomous-vehicles-matters/.

[90] K. Ngo, T. Mohammadat, J. Öberg, Towards a single event upset detector based on COTS fpga, in: Proceedings of the 2017 IEEE Nordic Circuits and Systems Conference, NorCAS-2017, IEEE, Linköping, Sweden, 2017.

[91] Mongelli, V. Orani, Stability certification of dynamical systems: Lyapunov logic learning machine, in: International Conference on Applied Soft Computing and Communication Networks, ACN'20, Springer, Chennai, India; Singapore, 2020.

[92] M. Mongelli, E. Ferrari, M. Muselli, A. Fermi, Performance validation of vehicle platooning through intelligible analytics, in: IET Cyber-Physical Systems: Theory &amp; Applications, (4) 2019, pp. 120–127.

[93] T. Decola, M. Marchese, M. Mongelli, F. Patrone, A Unified Optimisation Framework for QoS Management and Congestion Control in VHTS Systems, in: IEEE Transactions on Vehicular Technology.

[94] Ujcich, U. Thakore, W. Sanders, ATTAIN: An attack injection framework for software defined networking, in: 2017 47th Annual IEEE/IFIP Int. Conf. on Dependable Systems and Networks DSN, 2017, pp. 567–578.

[95] N. Neves, J. Antunes, M. Correia, P. Verissimo, R. Neves, Using attack injection to discover new vulnerabilities, in: Int. Conf. on Dependable Systems and Networks, IEEE, 2006, pp. 457–466.

[96] A. Avizienis, J.-C. Laprie, B. Randell, Fundamental concepts of dependability, 2001.

[97] K. Strandberg, T. Olovsson, E. Jonsson, Securing the connected car, IEEE vehicular technology magazine, March 2018, March 2018.

[98] M. Mongelli, M. Muselli, A. Scorzoni, E. Ferrari, Accellerating prism validation of vehicle platooning through machine learning, in: 2019 4th International Conference on System Reliability and Safety, ICSRS, IEEE, 2019, pp. 452–456.

[99] M. Mongelli, M. Muselli, E. Ferrari, Achieving zero collision probability in vehicle platooning under cyber attacks via machine learning, in: 2019 4th International Conference on System Reliability and Safety, ICSRS, IEEE, 2019, pp. 41–45.

[100] F. Smarra, A. D'Innocenzo, M.D. Di Benedetto, Fault tolerant stabilizability of MIMO multi-hop control networks, IFAC Proc. Vol. 45 (26) (2012) 79–84.

[101] F. Smarra, A. Jain, R. Mangharam, A. D'Innocenzo, Data-driven switched affine modeling for model predictive control, IFAC-PapersOnLine 51 (16) (2018) 199–204.

[102] T. Di Mascio, R. Gennari, A. Melonio, L. Tarantino, Supporting children in mastering temporal relations of stories: the TERENCE learning approach, Int. J. Dist. Educ. Technol. (IJDET) 14 (1) (2016) 44–63.

[103] Train Simulator - https://live.dovetailgames.com/live/train-simulator.

[104] Plone CMS - https://plone.org/.

[105] VALU3S YouTube Channel - https://www.youtube.com/channel/UCBvhaW8hkWgopiJWbFBrIFQ.

[106] World Health Organization, 'Coronavirus disease (COVID-19) pandemic' - https://www.who.int/emergencies/diseases/novel-coronavirus-2019.

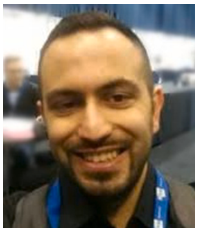
[107] https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy.

[108] https://aeneas-office.org/wp-content/uploads/2020/01/ECS-SRA2020{_}L.pdf.

[109] W. Afzal, H. Bruneliere, D. Di Ruscio, A. Sadovykh, S. Mazzini, E. Cariou, D. Truscan, J. Cabot, D. Field, L. Pomante, P. Smrz, The MegaM@Rt2 ECSEL Project: MegaModelling at Runtime — Scalable Model-Based Framework for Continuous Development and Runtime Validation of Complex Systems, in: 2017 Euromicro Conference on Digital System Design DSD4, 2017, pp. 94–501.

[110] L. Pomante, V. Muttillo, B. Krena, T. Vojnar, F. Veljković, P. Magnin, M. Matschnig, B. Fischer, J. Martinez, T. Gruber, The AQUAS ECSEL project aggregated quality assurance for systems: Co-engineering inside and across the product life cycle, Microprocess. Microsyst. 69 (2019).

[111] P. Castillejo, G. Johansen, B. Çürüklü, S. Bilbao, R. Fresco, B. Martínez-Rodríguez, L. Pomante, C. Rusu, J.-F. Martínez-Ortega, C. Centofanti, M. Hakojärvi, M. Santic, J. Häggman, Aggregate farming in the cloud: the AFarCloud ECSEL project, Microprocess. Microsyst. 78 (2020) 103218, http://dx.doi.org/10.1016/j.micpro.2020.103218.



Walter received his "Laurea Triennale" degree (BS) in 2014, his "Laurea Magistrale" (MS) in 2016 and a Ph.D in Computer Engineering at the University of L'Aquila, where he is currently working as postdoctoral researcher.

His research focuses on Cyber Security (both attack and defence), Embedded Systems platforms and protocols, Cryptography (cryptoanalysis, software and hardware implementations), Low-level software (e.g. OSs, Firmwares, Drivers etc.) analysis, reverse-engineering, digital hardware design and other topics.