The VALU3S ECSEL Project: Verification and Validation of Automated Systems Safety and Security

Abstract— **Manufacturers of automated systems and their components have been allocating an enormous amount of time and effort in R&D activities. 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 an ECSEL JU project (VALU3S) 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. 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.**

I. Introduction

The main effort in the development of automated systems is placed on a key factor: getting them to work. Between a prototype demonstrating new capabilities and a production version ready for the market, there are significant differences concerning quality properties such as safety and security. The quality properties of a system can be ensured through verification and validation procedures that take into account requirements such as safety, cyber-security, and privacy (SCP).

The focus of VALU3S is on verification and validation (V&V) of cyber-physical automated systems. To this aim, VALU3S will investigate 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. The initial dimensions of the framework are (i) the evaluation environment, (ii) type of evaluation, (iii) type of component under evaluation, (iv) the evaluation tool, (v) stage within the development process and (vi) the logic of the component under evaluation. Each dimension consists of multiple layers. For example, when it comes to the evaluation environment, the verification and validation process could be conducted in a (a) simulation environment, (b) a closed evaluation environment or (c) in an open environment (referred to as in-the-field).

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. 1, 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 Europes development in emerging areas mentioned in [4].

The starting day of the project is May 1st, 2020, and its duration is three years.

II. 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 gaps and limitations of cyber-physical systems by creating a list of SCP V&V 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 the gaps and limitations of existing methods in V&V of automated systems with 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) combination of methods that allows us to provide arguments and evidence for SCP of complex automated systems. This is part of the work to be done in the 3rd work package (WP) of the project.

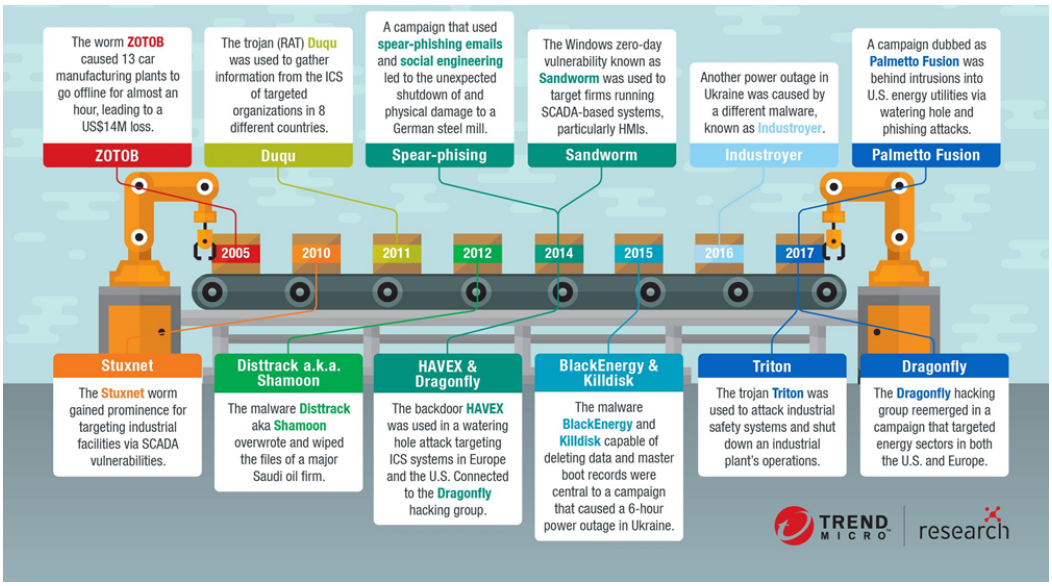

Fig. 1. Evolvement of security threats and risks over the past decades.

2) Development of a multi-layered framework for more effective verification and validation of automated systems with respect to SCP requirements of the VALU3S scenarios. This is part of the work to be done in WP2.
3) VALU3S will introduce a novel V&V workflow that is generic to reference methods in selected cyber-physical domains. This will be then complemented by the implementation of tools supporting the improved processes. In addition to the VALU3S repository of methods (WP3), the fulfillment of this objective is dependent on the VALU3S repository of scenarios (WP1), and detailed use case descriptions (WP1). This is part of the work to be done in WP4.
4) In total, 13 use cases from 6 domains, i.e. automotive, agriculture, railway, healthcare, aerospace and industrial robotics will be considered to demonstrate the strength of the proposed methodology concerning both SCP requirements, and time and cost of V&V processes. This is part of WP1 and WP5.
5) VALU3S will conduct a survey on state-of-the-art scenarios within each domain useful for evaluating SCP requirements of automated systems. This will be used to test and validate scenarios for SCP evaluation of the proposed methodologies. The list will be then extended to identify the gaps and limitations of existing scenarios with additional scenarios that take into account (i) scenarios that are defined specifically for automated system functionalities, and (ii) multi-domain scenarios including the ones that are applied to element out-of-context. This is part of the work to be done in WP1.
6) V&V tools and evaluation criteria will be developed in the qualification and quantification of SCP of systems under test. The evaluation criteria 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. This is part of the work to be done in WP4 and WP5.
7) To 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 standardisation 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. This is part of the work to be done in WP6.
8) 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. This is part of the work to be done in WP6.

III. Concept and Methodology

A. Concept

In the VALU3S project, we focus on 6 domains, i.e. automotive, agriculture, railway, healthcare, aerospace, industrial robotics/automation, studying a total of 13 use cases, described in Section IV, 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 [5], [6] 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, which is not a trivial task as system complexity rises dramatically with the more 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 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 (Fig. 2) 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. Six main properties (dimensions) consist of (i) the V&V evaluation environment, (ii) the type of evaluation chosen to be conducted, (iii) the type of component/system under evaluation, (iv) the tool that is used to conduct the evaluation, (v) the stage of evaluation i.e., whether the evaluation is a part of the verification process or a part of the validation process, and (vi) the logical category where the component/system is best represented in.

As shown in Fig. 2, 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. 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 V.

B. Methodology

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. This is done by designing and evaluating a multi-dimensional layered framework. VALU3S methodology consists of a four-step-process described in the remaining 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. This is why VALU3S aims to generate these test cases from commonly-used evaluation scenarios within the target domains. 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.
2) ***Creation of VALU3S repository of V&V methods.*** We plan to create 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 [7]) 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 tools 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.***

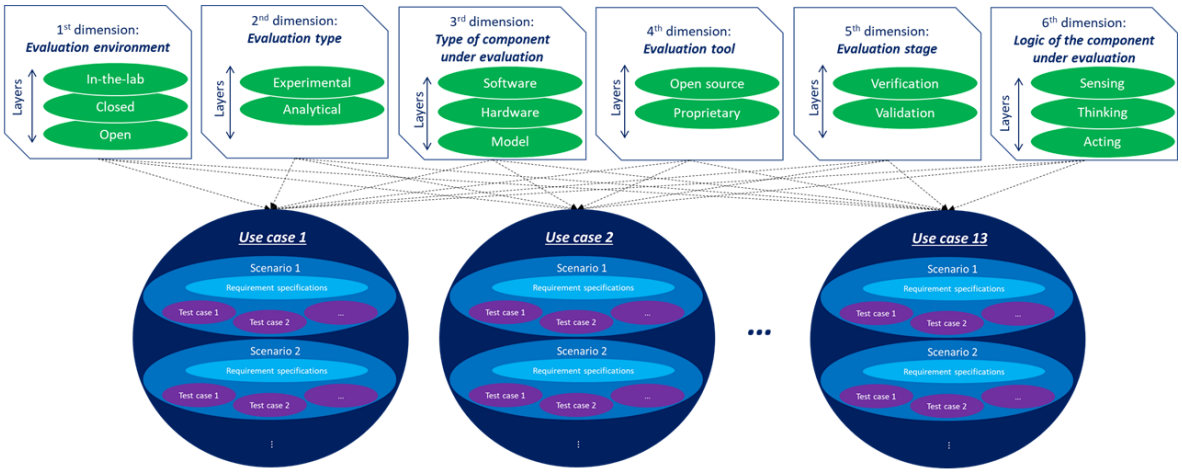

Fig. 2. VALU3S initial multi-dimensional layered framework.

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.

IV. VALU3S Use Cases

In the VALU3S project, 13 use cases are considered and are described in the following.

1) ***Intelligent Traffic Surveillance.*** Unicam 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. Currently, on the sites, Unicam systems are updated with CAMEA's smart cameras with the ability of running license 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 [8].
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. 3) - with drive by wire support. The car has six cameras installed on the roof.

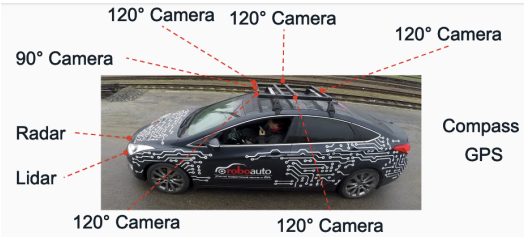

Fig. 3. Latest Roboauto model based on Hyundai i40.

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

system that allows quicker validation while increasing test coverage. Such a system is a radar system test bench which is placed in 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 ran 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 preprocessing, 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 [9], [10]. 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 form 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) proposes a use case that will cover automated fault and attack injection, specifically to control the aircraft engine (Fig. 4). 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. 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.
6) ***Agriculture robot.*** Energreen Company produces four multi utility and multi-tool teleoperated 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

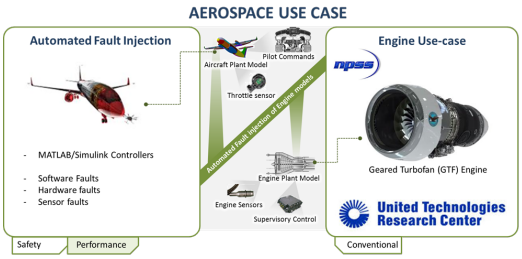

Fig. 4. UTRCI Aerospace use-case for automated fault-injection of engine models at simulation level

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 [11], [12], and their extension taking into account AI modelling techniques, such as [13].

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 Fundacin 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 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 on Computer Vision (CV) and Artificial Intelligence (AI) enhanced systems development to reach a higher autonomy in urban vehicles, and align them with railway European normative. The aim of these works is to apply CV&AI techniques to improve different autonomous train operation functionalities as precision stop, visual odometry, rolling stock coupling operation or person and obstacle detection-identification in railroads. CAF will use VALU3S approach to verify and validate some functionalities developed in CV & AI field for autonomous train operations, such as automatic platform detection for the automatic train approximation to accurate train stop, automatic accurate stop at door equipped platforms to align vehicle and platform doors, and doors management for safe passenger transfer. V&V procedures must consider that the system needs to be robust in presence of sensor malfunctions, platform detection and stopping mark pattern detection and segmentation malfunctions, camera calibration malfunctions, and AI algorithm malfunctions.
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. 5. 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. [14], [15] 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.

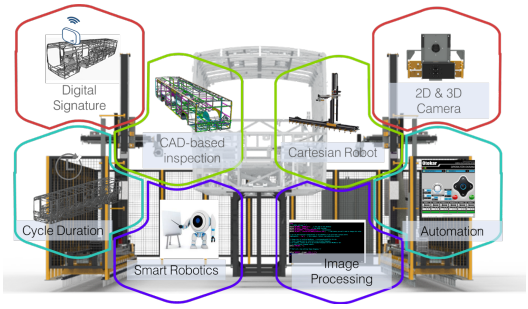

Fig. 5. The components of body-in-white inspection systems for world-selling OTOKAR buses.

12) ***Total Knee Arthroplasty navigation system. INCLUDE RUI'S FEEDBACK!!*** Total Knee Arthroplasty (TKA) is a surgical procedure to resurface a knee damaged by arthritis. Metal and plastic parts are used to cap the ends of the bones that form the knee joint (see Fig. 6). P3D is developing a marker-less

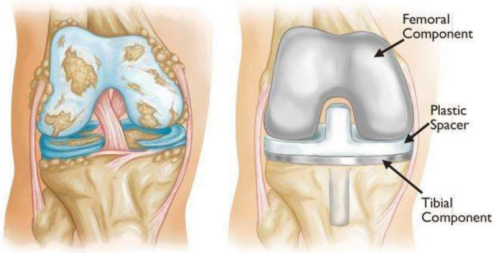

Fig. 6. (Left) pre-operative knee with severe arthritis; (right) post-operative knee with the implant.

navigation system that does not rely on any 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 marker-less 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.

V. Implementation

A. Work packages

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

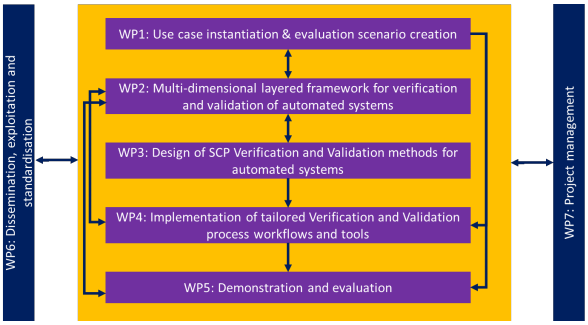

Fig. 7. Connection between different WPs in VALU3S

- ***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.
- ***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 VALU3S reference set of methods to be used for the V&V of automated systems. To do so, we plan to conduct 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.
- ***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.
- ***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 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.

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

B. 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. 8). 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).

VI. VALU3S Impact and alignment with EU Goals

As aligned with the EU goals formulated within the concept of Digital Single Economy [16], VALU3S fosters a horizontal solution stack supporting the effective exploitation of smart systems in all priority areas of ECS SRA 2020 [17].

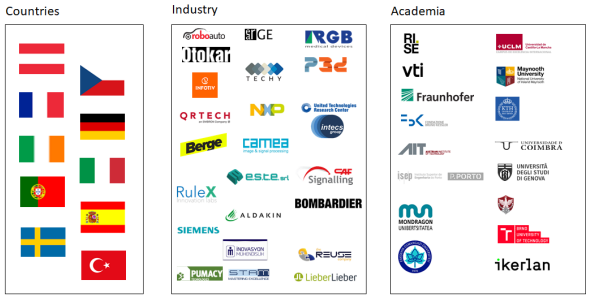

Fig. 8. VALU3S consortium.

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 EUs 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 labor saving will be provided, all of which will upgrade the working conditions.

VII. Conclusions

This paper has presented 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 on 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.

References

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

[2] Y. Z. Lun, A. DInnocenzo, F. Smarra, I. Malavolta, and M. D. Di Benedetto, "State of the art of cyber-physical systems security: An automatic control perspective," *Journal of Systems and Software*, vol. 149, pp. 174–216, 2019.

[3] A. D'Innocenzo, M. D. Di Benedetto, and 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] F. Smarra, G. D. Di Girolamo, V. De Iuliis, A. Jain, R. Mangharam, and A. DInnocenzo, "Data-driven switching modeling for mpc using regression trees and random forests," *Nonlinear Analysis: Hybrid Systems*, vol. 36, p. 100882, 2020.

[6] M. Mongelli and S. Scanzio, "A neural approach to synchronization in wireless networks with heterogeneous sources of noise," *Ad Hoc Networks*, vol. 49, pp. 1–16, 2016.

[7] B. Sangchoolie, P. Folkesson, and 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.

[8] L. Pomante, M. Pugliese, S. Marchesani, and 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.

[9] M. Mongelli, M. Muselli, A. Scorzoni, and 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.

[10] M. Mongelli, M. Muselli, and 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.

[11] L. Corradetti, D. Gregori, S. Marchesani, L. Pomante, M. Santic, and 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.

[12] F. Smarra, A. D'Innocenzo, and M. D. Di Benedetto, "Fault tolerant stabilizability of mimo multi-hop control networks," *IFAC Proceedings Volumes*, vol. 45, no. 26, pp. 79–84, 2012.

[13] F. Smarra, A. Jain, R. Mangharam, and A. DInnocenzo, "Data-driven switched affine modeling for model predictive control," *IFAC-PapersOnLine*, vol. 51, no. 16, pp. 199–204, 2018.

[14] L. Bozzi, L. Giuseppe, L. Pomante, M. Pugliese, M. Santic, F. Santucci, and 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.

[15] A. DInnocenzo, F. Smarra, and M. D. Di Benedetto, "Resilient stabilization of multi-hop control networks subject to malicious attacks," *Automatica*, vol. 71, pp. 1–9, 2016.

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

[17] https://aeneas-office.org/wp-content/uploads/2020/01/ECS-SRA2020_L.pdf.