

# VALU3S

*Verification and Validation of Automated Systems' Safety and Security*

## Final Demo

<b>Document Type</b>	Report
<b>Document Number</b>	D5.8
<b>Primary Author(s)</b>	Manuel Armin Schmidt (NXP)
<b>Document Date</b>	2023-05-26
<b>Document Version</b>	1.2 Final
<b>Dissemination Level</b>	Public (PU)
<b>Reference DoA</b>	2022-12-14
<b>Project Coordinator</b>	Behrooz Sangchoolie, <a href="mailto:behrooz.sangchoolie@ri.se">behrooz.sangchoolie@ri.se</a> , RISE Research Institutes of Sweden
<b>Project Homepage</b>	<a href="http://www.valu3s.eu">www.valu3s.eu</a>
<b>JU Grant Agreement</b>	876852



This 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.



### **Disclaimer**

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.

## Project Overview

Manufacturers of automated systems and the manufacturers of the components used in these systems have been allocating an enormous amount of time and effort in the past years to developing and conducting research on automated systems. The effort spent has resulted in the availability of prototypes demonstrating new capabilities as well as the introduction of such systems to the market within different domains. Manufacturers of these systems need to make sure that the systems function in the intended way and according to specifications which 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.

With rising complexity, unknown emerging properties of the system may come to the surface making it necessary to conduct thorough verification and validation (V&V) of these systems. Through the V&V of automated systems, the manufacturers of these systems are able to ensure safe, secure and reliable systems for society to use since failures in highly automated systems can be catastrophic.

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 in order to reduce the time and cost needed to verify and validate automated systems with respect to safety, cybersecurity and privacy (SCP) requirements. This ensures that European manufacturers of automated systems remain competitive and that they remain world leaders. To this end, a multi-domain framework is designed and evaluated 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.

In VALU3S, 13 use cases with specific safety, security and privacy requirements have been studied in detail. Several state-of-the-art V&V methods have been investigated and further enhanced in addition to implementing new methods aiming for reducing the time and cost needed to conduct V&V of automated systems. The V&V methods investigated are then used to design improved process workflows for V&V of automated systems. Several tools are implemented supporting the improved processes which are evaluated by qualification and quantification of safety, security and privacy as well as other evaluation criteria using demonstrators. VALU3S also influences the development of safety, security and privacy standards through an active participation in related standardisation groups. VALU3S provides guidelines to the testing community including engineers and researchers on how the V&V of automated systems could be improved considering the cost, time and effort of conducting the tests.

VALU3S brings together a consortium with partners from 10 different countries, with a mix of *industrial partners* (25 partners) from automotive, agriculture, railway, healthcare, aerospace and industrial automation and robotics domains as well as leading *research institutes* (6 partners) and *universities* (10 partners) to reach the project goal.

## Consortium

RISE RESEARCH INSTITUTES OF SWEDEN AB	RISE	Sweden
STAM SRL	STAM	Italy
FONDAZIONE BRUNO KESSLER	FBK	Italy
KNOWLEDGE CENTRIC SOLUTIONS SL - THE REUSE COMPANY	TRC	Spain
UNIVERSITA DEGLI STUDI DELL'AQUILA	UNIVAQ	Italy
INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO	ISEP	Portugal
UNIVERSITA DEGLI STUDI DI GENOVA	UNIGE	Italy
CAMEA, spol. s r.o.	CAMEA	Czech
IKERLAN S. COOP	IKER	Spain
CAF Signalling S.L	CAF	Spain
R G B MEDICAL DEVICES SA	RGB	Spain
UNIVERSIDADE DE COIMBRA	COIMBRA	Portugal
VYSOKE UCENI TECHNICKE V BRNE - BRNO UNIVERSITY OF TECHNOLOGY	BUT	Czech
ROBOAUTO S.R.O.	ROBO	Czech
ESKISEHIR OSMANGAZI UNIVERSITESI	ESOGU	Turkey
KUNGLIGA TEKNISKA HOEGSKOLAN	KTH	Sweden
STATENS VAG- OCH TRANSPORTFORSKNINGSINSTITUT	VTI	Sweden
UNIVERSIDAD DE CASTILLA - LA MANCHA	UCLM	Spain
FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V.	FRAUNHOFER	Germany
SIEMENS AKTIENGESELLSCHAFT OESTERREICH	SIEMENS	Austria
RULEX INNOVATION LABS SRL	RULEX	Italy
NXP SEMICONDUCTORS GERMANY GMBH	NXP-DE	Germany
PUMACY TECHNOLOGIES AG	PUMACY	Germany
UNITED TECHNOLOGIES RESEARCH CENTRE IRELAND, LIMITED	UTRCI	Ireland
NATIONAL UNIVERSITY OF IRELAND MAYNOOTH	NUIM	Ireland
INOVASYON MUHENDISLIK TEKNOLOJI GELISTIRME DANISMANLIK SANAYI VE TICARET LIMITED SIRKETI	IMTGD	Turkey
ERGUNLER INSAAT PETROL URUNLERI OTOMOTIV TEKSTIL MADENCILIK SU URUNLER SANAYI VE TICARET LIMITED STI.	ERARGE	Turkey
OTOKAR OTOMOTIV VE SAVUNMA SANAYI AS - OTOGAR AS	OTOKAR	Turkey
TECHY BILISIM TEKNOLOJILERI DANISMANLIK SANAYI VE TICARET LIMITED SIRKETI - TECHY INFORMATION TECHNOLOGIESAND CONSULTANCY LIMITED COMPANY	TECHY	Turkey
ELECTROTECNICA ALAVESA SL	ALDAKIN	Spain
INTECS SOLUTIONS SPA	INTECS	Italy
LIEBERLIEBER SOFTWARE GMBH	LLSG	Austria
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH	AIT	Austria
E.S.T.E. SRL	ESTE	Italy
NXP SEMICONDUCTORS FRANCE SAS	NXP-FR	France
BOMBARDIER TRANSPORTATION SWEDEN AB	BT	Sweden
QRTECH AKTIEBOLAG	QRTECH	Sweden
MONDRAGON GOI ESKOLA POLITEKNIKOA JOSE MARIA ARIZMENDIARRIETA S COOP	MGEP	Spain
INFOTIV AB	INFOTIV	Sweden
BERGE CONSULTING AB	BERGE	Sweden
CARDIOID TECHNOLOGIES LDA	CARDIOID	Portugal

## Executive Summary

This deliverable is part of Work Package 5 and presents the iterative process of demonstrator development of the project to guarantee a high maturity of the project results. The demonstrations of VALU3S will take place at the two final project events in Vienna (Austria) and Porto (Portugal). The major project results were merged to joint demonstrators (following called “lead demos”). The lead demos were presented during the 9<sup>th</sup> consortium meeting on the 4<sup>th</sup> of May, 2023, in Vienna, and will also be presented at the final project event in Porto on the 29<sup>th</sup> of June. This deliverable gives some impressions of the Vienna event and provides an outlook on the upcoming final demonstration. The deliverable focuses on giving an impression of the events through text, pictures, leaflets and posters.

This deliverable is composed of the preparation of the events with its planning (Chapter 2) and the best demonstrators (Lead Demos) of the Use Cases<sup>1</sup> (Chapter 3). Additionally, the conclusion is presented in Chapter 4, and all demonstrator posters will be shown in Appendix A. Each demonstrator is presented in a leaflet which is a summary of the project results (available to the public) and will be distributed and handed out at the event in Porto. Note that this deliverable is of type demonstration, however, in this report, we summarize the activities performed to demonstrate the project results.

---

<sup>1</sup> Except for UC12 since the UC provider terminated its participation in the project and UC14 was added by the lead partner CARDIOID.



## Contributors

Lukáš Maršík	CAMEA	Salih Ergün	ERARGE
Hamid Ebadi	INFOTIV	Aleš Smrčka	BUT
Thanh Bui	RISE	Martin Karsberg	INFOTIV
Jack Jensen	BERGE	Joakim Rosell	RISE
Bernhard Fischer	SIEMENS	Marie Farrell	NUIM
Jose Luis de la Vara	UCLM	Matt Luckcuck	NUIM
Arturo García	UCLM	Rosemary Monahan	NUIM
Giovanni Giachetti	UCLM	Oisin Sheridan	NUIM
Sina Borrami	ALSTOM	Gürol Çokünlü	OTOKAR
Håkan Palm	ALSTOM	Ömer Şahabaş	OTOKAR
Emanuele Mingozzi	ESTE	Muhammet Saral	OTOKAR
Katia Di Blasio	INTECS	Beata Davidova	ROBO
Stefano Tonetta	FBK	Ugur Yayan	IMTGD
Massimo Nazaria	FBK	Alim Kerem Erdogmus	IMTGD
Alberto Tacchella	FBK	Cem Baglum	IMTGD
Ludovico Battista	FBK	Lourenço Rodrigues	CARDIO
Metin Ozkan	ESOGU	Walter Tiberti	UNIVAQ
Ahmet Yazıcı	ESOGU	Luigi Pomante	UNIVAQ
Elif Değirmenci	ESOGU	Francesco Smarra	UNIVAQ
Yunus Sabri Kırca	ESOGU	Alessandro D'Innocenzo	UNIVAQ
Fabio Patrone	UNIGE	Davide Ottonello	STAM
Giovanni Gaggero	UNIGE	Florian Fischer	VTI
Georgios Giantamidis	UTRCI	Maytheewat Aramrattana	VTI
Xabier Mendiialdua	IKER	Mikel Aldalur	IKER
Íñigo Elguea	ALDAKIN	Stylianios Basagiannis	UTRCI
Krasen Parvanov	QRTECH	Nestor Arana	MGEP
Juan Manuel Morote	UCLM	Peter Folkesson	RISE
José Proença	ISEP	Bernd Bredehorst	PUMACY
Matt Luckcuck	NUIM	Zain Shawar	PUMACY
Marie Farrell	NUIM	Christoph Schmittner	AIT
Rosemary Monahan	NUIM	Mateen Malik	RISE
Oisín Sheridan	NUIM	Robert Sicher	LLSG
Alper Kanak	ERARGE	Clara Ayora	UCLM
Sercan Tanrıseven	ERARGE	Joseba Andoni Agirre	MGEP
Salih Ergün	ERARGE	Jose Pascual Molina	UCLM
Thomas Bauer	FRAUNHOFER	Ricardo Ruiz	RGB
	IESE		

## Reviewers

Aleš Smrčka	BUT	2023-05-22
Manuel Schmidt	NXP	2023-05-24
Lukáš Maršík	CAMEA	2023-05-22
Behrooz Sangchoolie	RISE	2023-05-24, 2023-05-25, 2023-05-26

## Revision History

Version	Date	Author (Affiliation)	Comment
0.1	2023-05-09	Manuel Schmidt (NXP)	Initial deliverable structure
0.2	2023-05-10	Manuel Schmidt (NXP)	Deliverable structure improved after comments of WP5 lead
0.3	2023-05-17	Manuel Schmidt (NXP)	Collected inputs from partners, ready for 1 <sup>st</sup> round of review.
0.4	2023-05-23	Manuel Schmidt (NXP)	An updated version reflecting reviewers' comments and suggestions
0.6	2023-05-24	Behrooz Sangchoolie (RISE)	Reviewing of the first draft of the report while making minor formatting changes and adding additional comments to be addressed.
1.0	2023-05-25	Manuel Schmidt (NXP)	Comments addressed.
1.1	2023-05-25	Behrooz Sangchoolie (RISE)	Reviewing of the second final draft of the report while making minor formatting changes.
1.2	2023-05-26	Behrooz Sangchoolie (RISE)	Final version of the report to be submitted.



# Table of Contents

Chapter 1	Introduction .....	15
Chapter 2	The Final Demonstration.....	17
2.1	The Consortium Meeting in Vienna.....	17
2.1.1	Preparations and Course of the event .....	17
2.2	The Final Project Event in Porto .....	22
2.2.1	Preparation and Course of the Event .....	22
Chapter 3	Demonstrators of Use Cases .....	25
3.1	Use Case 1 .....	26
3.2	Use Case 2.....	29
3.3	Use Case 3.....	31
3.4	Use Case 4.....	33
3.5	Use Case 5.....	37
3.6	Use Case 6.....	42
3.7	Use Case 7.....	46
3.8	Use Case 8.....	48
3.9	Use Case 9.....	52
3.10	Use Case 10.....	54
3.11	Use Case 11.....	56
3.12	Use Case 13.....	58
3.13	Use Case 14.....	60
Chapter 4	Conclusion.....	65
References	.....	67
Appendix A	Demo Posters .....	69
A.1	Use Case 1 .....	69
A.2	Use Case 2.....	71
A.3	Use Case 3.....	72
A.4	Use Case 4.....	73
A.5	Use Case 5.....	75
A.6	Use Case 6.....	79
A.7	Use Case 7.....	82



A.8	Use Case 8.....	83
A.9	Use Case 9.....	85
A.10	Use Case 10.....	86
A.11	Use Case 11.....	87
A.12	Use Case 13.....	88
A.13	Use Case 14.....	89

## List of Figures

Figure 2-1 Impressions from the venue.....	17
Figure 2-2 The introductory session on the morning of the first day was presented by Behrooz Sangchoolie (left) and the Austrian organizer Erwin Kristen (right).....	18
Figure 2-3 Some impressions of the 9th Consortium Meeting in Vienna. ....	19
Figure 2-4 Poster template of the demonstrators.....	21
Figure 2-5 Some impression of the place where the final project event in Porto .....	22



# List of Tables

Table 2-1 List of Lead Demonstrators with their responsibilities ..... 19

Table 2-2 Links to the pitch videos ..... 23



## Acronyms

ADAS	Advanced Driver-Assistance System
AI	Artificial Intelligence
CAD	Computer Aided Design
CI	Continuous Integration
CIS	Computer Interlocking System
CV	Computer Vision
Demo	Demonstrator
DSN	Dependable Systems and Networks
ECG	Electrocardiogram
FLA	Failure Logic Analysis
FMEA	Fault Mode and Effects Analysis
FT	Fault Trees
HiL	Hardware-In-the-Loop
HRI	Human-Robot-Interaction
IC	Integrated Circuit
IMU	Inertial Measurement Unit
IP	Intellectual Property
KCSE	Knowledge-Centric Systems Engineering
ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
MSA-FLA	Model-based Safety Analysis with Failure Logical Analysis
NMT	Neuro Muscular Transmission
PLC	Product Life-Cycle
QEMU	Quick Emulator
RAMS	Reliability, Availability, Maintainability and Safety
SCP	Safety, Cybersecurity, and Privacy
SIL	Safety Integrity Level
SiLVer	Simulation-based Verification
UC	Use Case
V&V	Verification and Validation
VR	Virtual Reality
WP	Work Package

# Chapter 1 Introduction

One of the main objectives of the VALU3S project was to lower the effort and cost of engineering processes by focusing on one (or more) of the most resource-consuming steps of the product life cycle – verification and validation (V&V). V&V is not just a single engineering phase, but a complex process integrated into different engineering phases, applied in different levels of details of development. It begins before even a single line of code is produced and does not end after a product is deployed to the market. The VALU3S project aims at V&V of automated systems, which require special approaches in providing confirmation of services and warranties which are different from the traditional techniques. Within the project, a V&V framework has been developed, which integrates newly proposed and/or improved versions of already existing V&V methods and tools supporting these methods. The framework has been applied in the development phase of products in different domains (agriculture, aerospace, automotive, healthcare, industrial robotics, and railway) to show the improvements gained by the framework. The V&V process is being improved not just by reducing the effort and cost but also by increasing the quality of products while reducing the time needed for V&V. This main result has been demonstrated within intermediate demonstrations and have been finalised at the end of the project by providing an evaluation report for all demonstrators in all use cases in D5.6 [1] and by demonstrating the utilization of newly developed methods and tools in these use cases.

The purpose of this document is to present the lead demonstrators, which have been presented during the demonstration events in Vienna (Austria) and will be presented in the Final Demo session in Porto (Portugal). The lead demos were presented during the 9<sup>th</sup> consortium meeting & general assembly & 1st RP3 review rehearsal on the 4<sup>th</sup> May, 2023, in Vienna. Moreover, the lead demos will also be presented at the final project event in Porto on the 29<sup>th</sup> of June. In order to finalise the project in time and to provide the reviewers with the possibility to review every deliverable before the final (RP3) review meeting on 28<sup>th</sup> of June, most impressions in the following chapters are mainly from the demo event in Vienna (Austria), but the final event in Porto (Portugal) will follow the same structure. The demonstration consists of several so-called *demonstrators*, which are prepared by different Use Case (UC) contributors and validated in the target domain of the individual UC provider. As detailed descriptions of the demonstrators is listed in the two deliverables D5.5 [2] and D5.6 [1], this report focuses on the demo events as well as the communication material used to present the results of the project results to the public. To share the greatest impressions of the events, pictures from Vienna, the demo communication material such as leaflets and posters are shown in this deliverable. Moreover, the preparations for the events in Vienna and Porto are listed as well.





## Chapter 2 The Final Demonstration

The lead demos were showcased at the 9<sup>th</sup> consortium gathering on May 4<sup>th</sup>, 2023, in Vienna, and are scheduled to be displayed at the project's concluding event in Porto on June 29<sup>th</sup>, 2023. Because of the timeline, the following sections primarily reflect the Vienna event, but the Porto event will be of a similar nature. The planning and progression of both events, held in Vienna and Porto, are outlined. Central themes of the events include presentations on Work Packages 2, 4, 5, and 6, as well as "Market, competition, and exploitation plans from all partners", with a special emphasis on the unveiling of the Lead Demonstrators. In preparation for this, posters were made ahead of time to display the content of the demos and their impacts in a nutshell (see Appendix A). For the Porto event, additional leaflets for each UC have been created and will be handed out on location (see Chapter 3).

### 2.1 The Consortium Meeting in Vienna

#### 2.1.1 Preparations and Course of the event

The VALU3S 9<sup>th</sup> Consortium Meeting (includes also general assembly & 1st RP3 review rehearsal) was organized as a two-day meeting on 3<sup>rd</sup> and 4<sup>th</sup> of June 2023 in Vienna, Austria. On the day of the event, the rooms were prepared for the meetings in the Hotel NH Donau City (see Figure 2-1). For the presentations and speeches on the first day, there was one room furnished with a projector and a lectern. The demonstrations were presented on the second day in a separate room equipped with several laptops and pinboards.

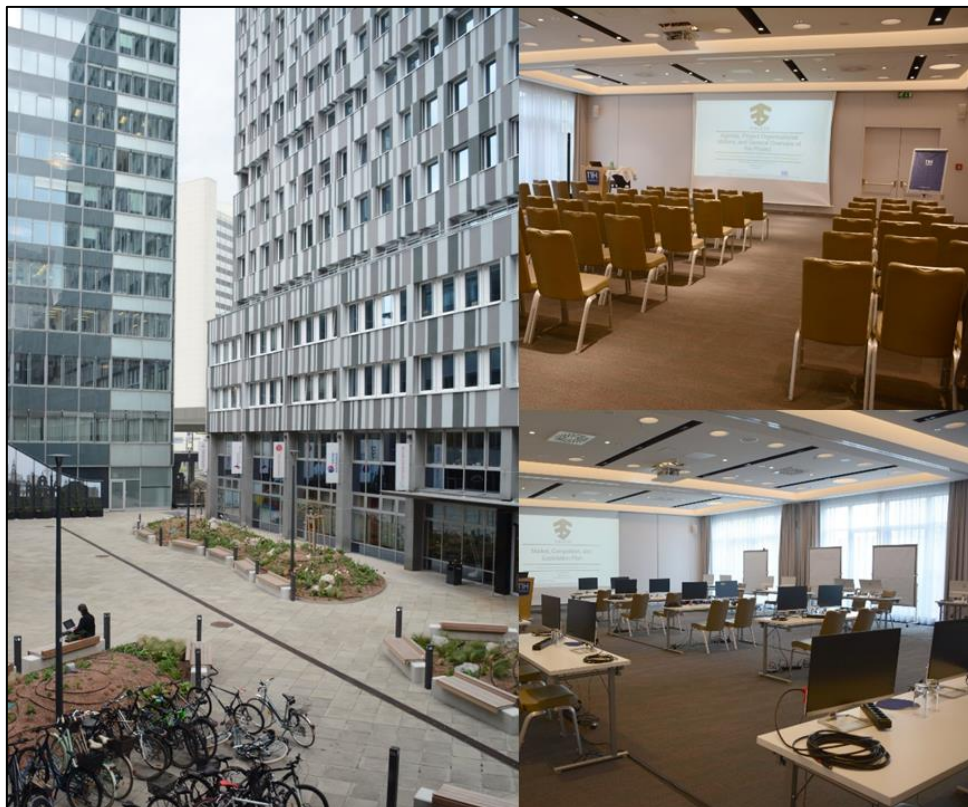


Figure 2-1 Impressions from the venue.

### *Presentations on the first day*

After the registration on the first day, the project coordinator Behrooz Sangchoolie introduced the participants, welcomed everyone and presented the agenda for the following days (see Figure 2-2). Further points were addressed, such as the financial and technical report or gender balance and diversity. As mentioned before, the key topics of the event were the presentations of Work Packages 2, 4, 5 and 6, and “Market, competition and exploitation plans of all partners” .



*Figure 2-2 The introductory session on the morning of the first day was presented by Behrooz Sangchoolie (left) and the Austrian organizer Erwin Kristen (right).*

### *Demonstrations on the second day*

On the second day, after a preparation of the demonstration site, a short pitch session started in which each demonstrator had the chance to introduce the booth to the partners (2 minutes per demonstrator, compare the upper picture on the right side, and bottom picture on the left side of Figure 2-3). Finally, the demonstration was held, which constituted the main program (bottom picture on the left side). Here, partners had the chance to go around the booths, discuss the project results with the partners, provide feedback, learn and to discover future opportunities.



Figure 2-3 Some impressions of the 9th Consortium Meeting in Vienna.

In total 22 lead demonstrators were developed by the project consortia in 13 use cases and the six ECR target domains (see Table 2-1).

Table 2-1 List of Lead Demonstrators with their responsables.

	Demonstrator name	Responsible(s) / Contact(s)	UC
<b>Demo-1</b>	Verification and validation of an automated robot inspection cell for automotive body-in-white	Gurol Cokunlu (Otokar) Ahmet Yazıcı (ESOGU)	UC11
<b>Demo-2</b>	Remote controlled radar target simulation and validation	Manuel A. Schmidt (NXP)	UC3
<b>Demo-3</b>	Data Generation and Validation for Railway domain	Mikel Aldalur (IKER)	UC9
<b>Demo-4</b>	Coordination of Test Generation and Validation in Simulation based Human-Robot Collaborative environments	Joseba A. Agirre (MGEP) Íñigo Elguea (ALDAKIN)	UC7
<b>Demo-5</b>	NMT Simulator	Martin Hruby (BUT) and Ricardo Ruiz (RGB)	UC8
<b>Demo-6</b>	Mu-FRET	Rosemary Monahan (NUIM)	UC5
<b>Demo-7</b>	Testing and Verification of Remotely Operated Vehicles (ROV) Safety by injecting Faults and Attacks in the Wi-Fi based communication system	Mateen Malik (RISE) Maytheewat Aramrattana (VTI)	UC2
<b>Demo-8</b>	V&V of ML based vehicle detection traffic system using simulators	Thanh Bui, Joakim Rosell (RISE), Hamid Ebadi (Infotiv), Jack Jenssen (Berge)	UC1

	Demonstrator name	Responsible(s) / Contact(s)	UC
Demo-9	Hardware in-the-Loop Validation Station	Lourenço Rodrigues, José Santos (CardioID), Giann Nandi (ISEP), Frederico Cerveira (COIMBRA)	UC14
Demo-10	Instrumented Driving Simulator for drowsiness data generation	Lourenço Rodrigues (CardioID), Maytheewat Aramrattana (VTI)	UC14
Demo-11	Real-Time Analogue Signal Monitoring (RTAMT) for a Digital Twin for Motion Control	Bernhard Fischer (Siemens), Dejan Nickovic (AIT), Erwin Kristen (AIT)	UC13
Demo-12	Early V&V in Knowledge-Centric Systems Engineering	Jose Luis de la Vara (UCLM), Luis Alonso (TRC), Juan Manuel Morote (UCLM), Ricardo Ruiz (RGB)	UC8
Demo-13	Safety verification and validation for the signalling railway application	Sina Borrami (Alstom), Jonas Melchert (Alstom), José Proença (ISEP) Erwin Kristen (AIT), Robert Sicher (LieberLieber)	UC10
Demo-14	MSA-FLA with CHES-FLA	Katia Di Blasio (INTECS)	UC6 & UC8
Demo-15	Arm Unity	Emanuele Mingozzi (ESTE)	UC6
Demo-16	Model-based Design and Validation of the Hybrid Model	Stefano Tonetta (FBK)	UC5
Demo-17	Pre-injection analysis for model-implemented fault- and attack injection	Peter Folkesson (RISE)	UC5
Demo-18	Handling and gripping of product/parts	Zain Shahwar (PUMACY), Bernd Bredehorst (PUMACY), Thomas Bauer (FHG), Iron Prandoda Silva (FHG)	UC4
Demo-19	ML-Pipeline	Zain Shahwar (PUMACY), Bernd Bredehorst (PUMACY), Thomas Bauer (FHG), Iron Prandoda Silva (FHG)	UC4
Demo-20	Testing network communication using NetLoiter	Ales Smrcka (BUT)	UC1 & UC2
Demo-21	Simulation-based Verification (SiLVer) workflow & tool	Georgios Giantamidis (UTRCI), Stylianos Basagiannis (UTRCI)	UC5
Demo-22	RAMSES tool for Risk Management of Agriculture Robot	Davide Ottonello (STAM)	UC6

## Demonstration Material

The partners were free to choose their style of demonstration, but nevertheless, the demonstration setup for most of the demonstrators consisted of three elements. Each demonstrator had a screen on which live demos, videos or further explanations could be displayed. Further, there was space for partners to present hardware equipment. In addition to that, posters were prepared to summarise the most important takeaways such as the connected tools, a link to the workflow of the demonstrator in the web repository and the quantitative evaluations as well as their impacts on the automation of V&V. The layout of the poster can be seen in Figure 2-4. The demo posters of Vienna are displayed in Appendix A.

Placeholder for Application Domain Icon

Developed in Use Case: Use Case No.



# Demonstrator Title

### Name of the selected demonstrator

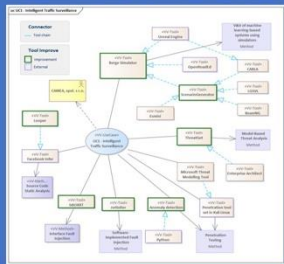
Short textual description of the demonstrator



### Connection of the tool(s)

Short description of the tool(s) of the demonstrator and/or connection of the tools in a toolchain. If space left, please add 2-3 bullets on the interrelation of the tools

Diagram from EA (which shows the tool relations)



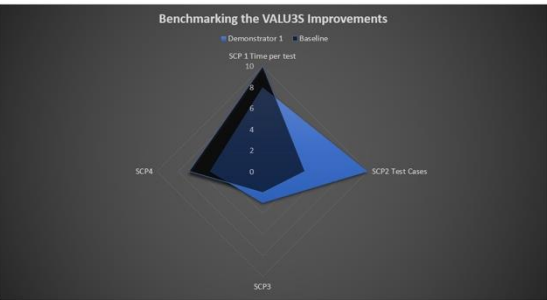
If space, please add 2-3 bullets about the interrelation of the tools

Workflow of the UC (QR Code to Web repo)



### Evaluation

Description about the evaluation connected to the demonstrator.



### Expected Impacts

- Expected impact 1 by improvement x
- Expected impact 2 by improvement y
- ...

### Related/ Impacted Standards

- Standard ID1: Description of the relation/ How is the Standard impacted by the demonstrator development?
- Standard ID2: Description of the relation/ How is the Standard impacted by the demonstrator development?

### Involved VALU3S Partners

Leader: Participating Partners:

VALU3S HAS RECEIVED FUNDING FROM THE ECSEL JOINT UNDERTAKING UNDER GRANT AGREEMENT NO 876852. THE JOINT UNDERTAKING RECEIVES SUPPORT FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME AND AUSTRIA, CZECH REPUBLIC, GERMANY, IRELAND, ITALY, PORTUGAL, SPAIN, SWEDEN, TURKEY.



Figure 2-4 Poster template of the demonstrators

## 2.2 The Final Project Event in Porto

### 2.2.1 Preparation and Course of the Event

The VALU3S Final Project Event is a two-day meeting from 28<sup>th</sup> to 29<sup>th</sup> June 2023 in the Palácio da Bolsa in Porto, Portugal. Palácio da Bolsa was the Porto stock exchange building in the XIX century. VALU3S meeting room is Auditorium António Calém on the 2<sup>nd</sup> floor of Palácio da Bolsa. Some impressions of the venue of the final demo can be seen in Figure 2-5.



*Figure 2-5 Some impression of the place where the final project event in Porto*

VALU3S Final Project Event is collocated with the 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2023) in Porto (Portugal, 27-30 of June 2023). In particular, the VALU3S Demonstration session on 29 of June will be included in the DSN 2023 official program, which represents an excellent opportunity for the dissemination of VALU3S results in the world's top conference on computer dependability and security (DSN 2023). The first day of the conference (27 of June) includes the Workshop on the Verification & Validation of Dependable Cyber-Physical Systems (VERDI) proposed by VALU3S researchers.

The first day of the event will still be closed for the public. On the first day, the partners will have the final project update and retro perspective of the performed work in the 3<sup>rd</sup> year review meeting in which the current state of the project and the remaining deliverables are discussed. The second day will be public and a great chance to show the final project results to the visitors.

#### **Demonstration Material**

In addition to the software (screen), hardware demonstrators and posters, two new formats were created to provide the visitors with the best experience of the project results. On the one hand, leaflets were created, which will be available at each booth for takeaway and contain the most critical information of the lead demos, some impressions and a possibility to contact the demonstrator leader.

Thus, the leaflet has the function of a demonstrator business card which enables dissemination also after the project ends. On the other hand, short pitch videos of each demonstrator are created, which will be uploaded to the web repository and give the viewer a brief explanation of the demo in case, e.g., the visitor wants to remember what exactly the demos were about. This provides a convenient way to stay in mind of the visitors.

All leaflets combined will be forming a booklet of the project outcomes presented in Chapter 3 and available on the web-based repository [3].

The leaflet is started with a rough overview of the project. Afterwards, the demonstrators are structured by use case. There is always one UC overview, which describes the demonstration domain and its challenges which the demonstrators resolve. Additionally, each lead demo has a descriptive slide which includes information on how it solves the challenges, some impressions, a link to the video pitches and the evaluation results. The demonstrator overview plus the specific demonstrator descriptions form each leaflet (and consequently as many leaflets as UCs). The leaflets are listed in Chapter 3.

As described before, most of the demonstrators also created pitch videos. A few demonstrators were unfortunately not able to share a video as of now due to company restrictions. The videos can be accessed via the links in Table 2-2:

Table 2-2 Links to the pitch videos

Demo #	Demonstrator name	Link to pitch video
UC1		
Demo-8	V&V of ML based vehicle detection traffic system using simulators	<a href="https://www.youtube.com/watch?v=ti4yRIKBGyI&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=7">https://www.youtube.com/watch?v=ti4yRIKBGyI&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=7</a>
Demo-20	Testing network communication using NetLoiter	<a href="https://www.youtube.com/watch?v=7T3iQqw9dWM&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=19">https://www.youtube.com/watch?v=7T3iQqw9dWM&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=19</a>
UC2		
Demo-7	Testing and Verification of Remotely Operated Vehicles (ROV) Safety by injecting Faults and Attacks in the WiFi based communication system	<a href="https://www.youtube.com/watch?v=7T3iQqw9dWM&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=19">https://www.youtube.com/watch?v=7T3iQqw9dWM&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=19</a>
UC3		
Demo-2	Remote controlled radar target simulation and validation	N/A
UC4		
Demo-18	Handling and gripping of product/parts	<a href="https://www.youtube.com/watch?v=5qKZDhkFQHc&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=17">https://www.youtube.com/watch?v=5qKZDhkFQHc&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=17</a>
Demo-19	ML-Pipeline	Joint demo with Demo18
UC5		
Demo-6	Mu-FRET	<a href="https://www.youtube.com/watch?v=5qKZDhkFQHc&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=17">https://www.youtube.com/watch?v=5qKZDhkFQHc&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=17</a>
Demo-16	Model based Design and Validation of the hybrid Model	<a href="https://www.youtube.com/watch?v=5qKZDhkFQHc&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=17">https://www.youtube.com/watch?v=5qKZDhkFQHc&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=17</a>
Demo-17	Pre-injection analysis for model-implemented fault- and attack injection	<a href="https://www.youtube.com/watch?v=dIGq5K3fO6o&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=16">https://www.youtube.com/watch?v=dIGq5K3fO6o&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=16</a>
Demo-21	Simulation-based Verification (SiLVer) workflow & tool	N/A



Demo #	Demonstrator name	Link to pitch video
UC6		
Demo-14	MSA-FLA with CHES-FLA	<a href="https://www.youtube.com/watch?v=SB3ViNODPGs&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=13">https://www.youtube.com/watch?v=SB3ViNODPGs&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=13</a>
Demo-15	Arm Unity	<a href="https://www.youtube.com/watch?v=wXM2JH162wc&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=14">https://www.youtube.com/watch?v=wXM2JH162wc&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=14</a>
Demo-22	RAMSES tool for Risk Management of Agriculture Robot	<a href="https://www.youtube.com/watch?v=z0ueYaxF1_g&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=19">https://www.youtube.com/watch?v=z0ueYaxF1_g&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=19</a>
UC7		
Demo-4	Coordination of Test Generation and Validation in Simulation based Human-Robot Collaborative environments	<a href="https://www.youtube.com/watch?v=qxscy9p3_i0&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=4">https://www.youtube.com/watch?v=qxscy9p3_i0&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=4</a>
UC8		
Demo-5	NMT Simulator	<a href="https://www.youtube.com/watch?v=qxscy9p3_i0&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=4">https://www.youtube.com/watch?v=qxscy9p3_i0&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=4</a>
Demo-12	Early V&V in Knowledge-Centric Systems Engineering	<a href="https://www.youtube.com/watch?v=qxscy9p3_i0&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=4">https://www.youtube.com/watch?v=qxscy9p3_i0&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=4</a>
UC9		
Demo-3	Data Generation and Validation for Railway domain	<a href="https://www.youtube.com/watch?v=HjvZPX-IA-U&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=2">https://www.youtube.com/watch?v=HjvZPX-IA-U&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=2</a>
UC10		
Demo-13	Safety verification and validation for the signaling railway application	<a href="https://www.youtube.com/watch?v=cmKzNP5S1Is&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=12">https://www.youtube.com/watch?v=cmKzNP5S1Is&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa&amp;index=12</a>
UC11		
Demo-1	Verification and validation of an automated robot inspection cell for automotive body-in-white	<a href="https://www.youtube.com/watch?v=ub80FboyJHA&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa">https://www.youtube.com/watch?v=ub80FboyJHA&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa</a>
UC13		
Demo-11	Real-Time Analogue Signal Monitoring (RTAMT) for a Digital Twin for Motion Control	<a href="https://www.youtube.com/watch?v=ub80FboyJHA&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa">https://www.youtube.com/watch?v=ub80FboyJHA&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa</a>
UC14		
Demo-9	Hardware in-the-Loop Validation Station	<a href="https://www.youtube.com/watch?v=ub80FboyJHA&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa">https://www.youtube.com/watch?v=ub80FboyJHA&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa</a>
Demo-10	Instrumented Driving Simulator for drowsiness data generation	<a href="https://www.youtube.com/watch?v=ub80FboyJHA&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa">https://www.youtube.com/watch?v=ub80FboyJHA&amp;list=PLGtGM9euw6A6FYkAatzU9YPB1RkSEM4Aa</a>



## Chapter 3 Demonstrators of Use Cases

This chapter presents the lead demonstrators of all UCs<sup>2</sup> as leaflets. The leaflets will be used at the Final Project Event in Porto and uploaded in the web repository.

### Verification and Validation of Automated Systems' Safety and Security



#### About the Project

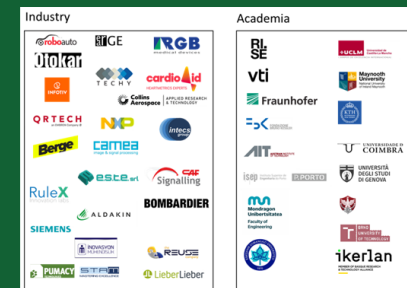
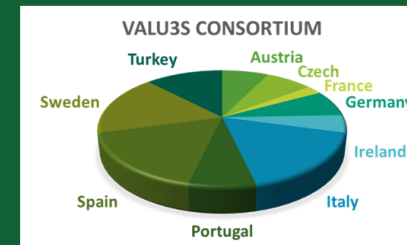
The high complexity of an automated system incurs overhead on the Verification and Validation process, making it time-consuming and costly.

VALU3S aimed to design, implement and evaluate state-of-the-art Verification and Validation methods and tools that reduce the time and cost needed to verify and validate automated systems with respect to safety, cybersecurity and privacy requirements.

At the VALU3S Final Demo session, **22 demonstrators** are showcased. The demonstrators have been built on top of **13 project Use Cases** from **six domains** of agriculture, aerospace, automotive, healthcare, industrial robotics, and railway.

#### The consortium

- The consortium consists of 41 project organisations from 10 countries.
- The total Horizon 2020 project cost is ~25 857 454 €.



<sup>2</sup> Except for UC12 since the UC provider terminated its participation in the project and UC14 was added by the lead partner CARDIOID.

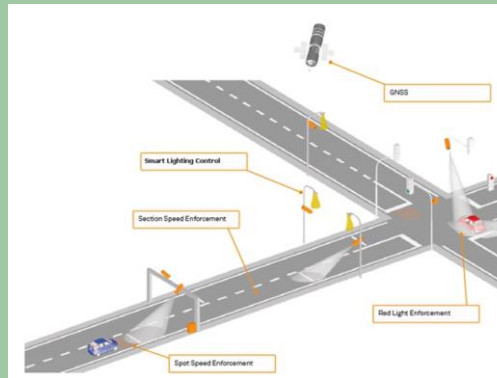
### 3.1 Use Case 1

# Demonstrations of UC1 - Intelligent Traffic Surveillance



## Use Case Description

UC1 from CAMEA focuses on the intelligent traffic monitoring system based on camera/radar perception sensors. The example subsystem selected in the UC is License Plate Detection.



## Challenges addressed by the lead demonstrators

- Radar/camera-advanced detection and tracking system uses ML component(s), which is data-driven and opaque.
- Data for V&V of the system's performance and robustness are not feasible to capture only from real-world settings

## Demonstrations

- 1) V&V of Vehicle/LP detection using a simulator (Lead demo)
- 2) Testing network communication using NetLoiter (Lead demo)
- 3) Integration of threat modelling and penetration testing (Complementary)

UC1 in the web repository



## V&V of Vehicle/LP detection using simulator

This showcases a photo-realistic Berge Simulator to model traffic scenarios for V&V of the CAMEA ML-based LP recognition system. This has been verified by feeding simulated inputs to core processing components used in real traffic monitoring systems and comparing detection results with those obtained based on the real data input.

### Link to demo pitch video



### Contact person for the demo

Joakim Rosell  
(joakim.rosell@ri.se)

## Impressions

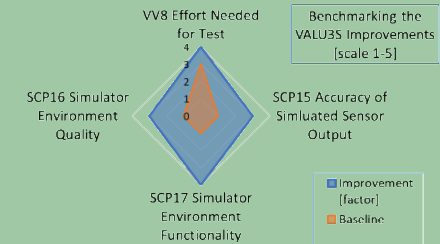
Real image of “Åkareplatsen resecentrum” in Gothenburg, Sweden and Corresponding synthetic scene generated in the Berge simulator.



Example images from the Berge simulator where the addition of waypoints and agents are shown.



## Improvement and Impact



- Reduction of development costs, improved reliability, and faster time-to-market.
- Easier testing and validation of traffic monitoring and quality inspection systems.
- Simplified modification and customisation of traffic monitoring systems.
- Automation during continuous integration/development.

### Participating partners



## NetLoiter

Demonstration of a systematic way of injecting faults into network traffic using a newly developed tool NetLoiter. The tool is used for experiments in test cases related to checking if a system-under-test performs correctly under different network conditions. Faults (i.e. unexpected conditions of network traffic) include network latency, lossy channel, packet reordering, jitter, and/or their combinations.

### Link to demo pitch video

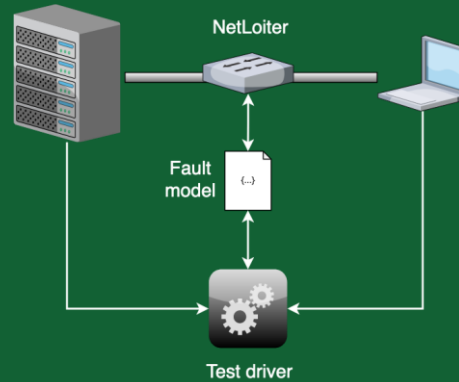


### Contact person for the demo

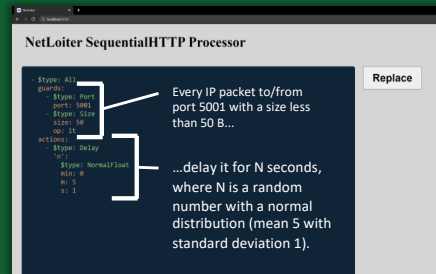
Ales Smrcka  
(smrcka@vutbr.cz)

## Impressions

Scheme of the NetLoiter intercepting the connection between two computers or IoT devices.

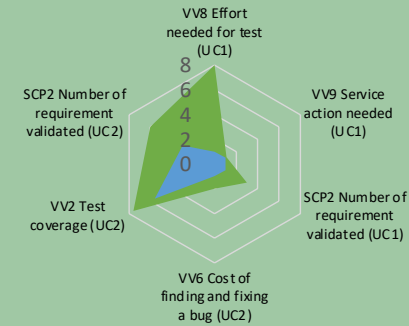


NetLoiter can be configured during run-time, which enables automated search-based testing – NetLoiter can search for the worst network conditions under which the tested application works properly.



## Improvement and Impact

■ Demonstrator [factor] ■ Baseline



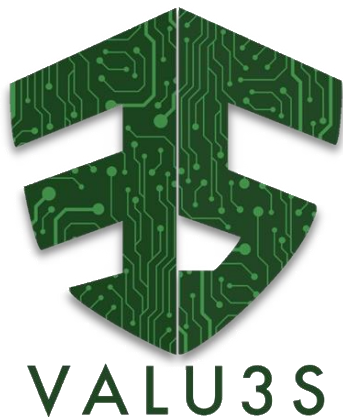
NetLoiter has been used for evaluating the resilience of applications remotely controlling the radar (in the case of UC1) and for a vehicle (in the case of UC2). Such kind of testing significantly reduces the time and effort spent on V&V activities.

### Participating partners



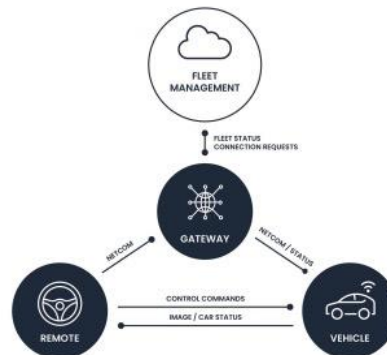
### 3.2 Use Case 2

# Demonstrators of Use Case 2 - Car Teleoperation



## Use Case Description

Use case 2 from Roboauto focuses on the cybersecurity of the transmission line and the routers to ensure the safety of the car and its passengers in car teleoperation.



## Challenges addressed by the lead demonstrators

- Evaluation of the correct simulated car behaviour in case of a fault or an attack on communication lines.
- Reduction of effort (time and cost) in testing changes in the teleoperation system.

## Demonstrations

- 1) V&V of Car Teleoperation application under Faults and Attack in Wireless Communication Channel (Lead)
- 2) Testing network communication using NetLoiter (Lead)
- 3) Integration of threat modelling and penetration testing (Complementary)

## UC in the web repository



## V&V of Car Teleoperation application under Faults and Attacks in wireless communication

ComFASE is a communication-based fault and attack injection tool developed to inject faults and attacks in communication between modules of the car teleoperation system (UC2 mock-up) to verify and validate the safety features implemented in the car teleoperation system.

For this purpose, the car teleoperation modules provided by the UC provider (i.e., Gateway, Remote station, Car, and ECU) are connected to Veins\_INET—framework simulation of wireless communication. This framework is then used to test the functional requirements of the system.

The complete simulation environment and the physical test setup are provided here.

### Link to demo pitch video

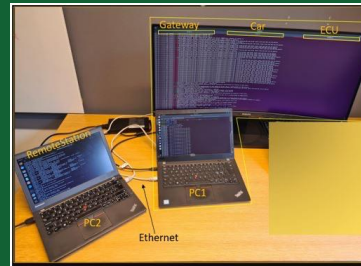


### Contact person for the demo

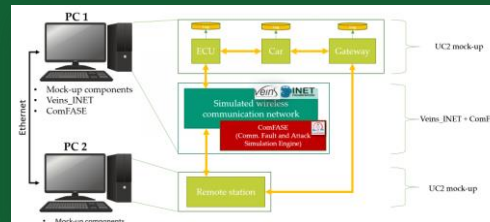
Mateen Malik  
(mateen.malik@ri.se)

## Impressions

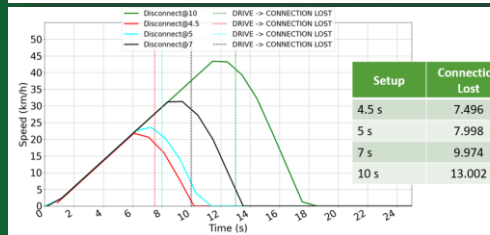
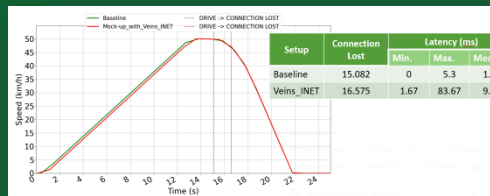
Physical test setup for verification and validation of the UC2 teleoperation system



UC2 Demonstrator Implementation with Simulated Network



### Simulation Results



## Improvement and Impact



The above chart represents the improvement of the verification and validation of the teleoperation system in terms of time. The time required to prepare a test setup for executing tests can vary depending on whether real-world or simulation-based testing is employed.

Real-world testing necessitates the use of actual vehicles, and the creation of a safe test environment, whereas simulation-based testing eliminates these concerns. However, setting up a realistic simulation-based test environment can be challenging depending on the system's complexity.

Considering the above test setup and execution needs, we estimated that the test to verify the teleoperation system's functional requirement in the real world takes one day (i.e., 8 hours) to run all tests in the real world. The time distribution looks approximately this, 3 hours of preparation (prepare, leave office, get the car), 2 hours of testing (for all tests), and 1 hour for closure. So, one test takes roughly 96 minutes to complete.

It takes to execute the same test in a simulation-based environment roughly 30 minutes or less.

### Participating partners



### 3.3 Use Case 3

## Demonstrators of Use Case 3 - Radar System for ASAS



### Use Case Description

**Use Case 3** addresses the need for complexity reduction and efficiency improvement of the existing V&V process by new tools and methods. The use case tests these tools in the environment of validating modern ADAS systems from an ADAS IC manufacturer perspective.



### Challenges addressed by the lead demonstrators

- Validation ends after unit testing, and thus, radar system bugs are often detected late
- There is limited access to expensive test equipment

### Demonstrations

- 1) Remote controlled radar target simulation and validation (Lead)
- 2) Validation of silicon chips integrated in a corner radar system (Complementary)

### UC in the web repository



## Remote controlled radar target simulation and validation

The **lead demonstrator** of UC3 focuses on demonstrating a first approach to implementing such system testing in the V&V workflow. Especially the simulation of system components and real-world driving scenarios can play a vital role. Therefore, this demonstrator covers mainly the integration of the RSES (Radar System Environment Simulator) in the V&V workflow.

### Contact person for the demo

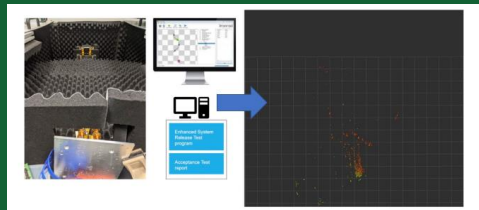
Manuel Schmidt  
(manuel.Schmidt@nxp.com)

## Impressions

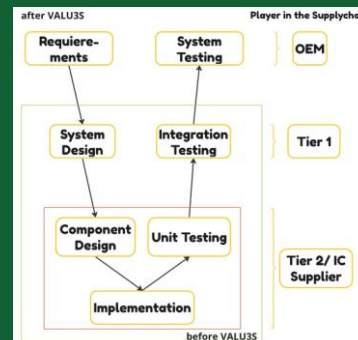
GUI from the RSES showing a traffic scenario with two moving targets with different velocity



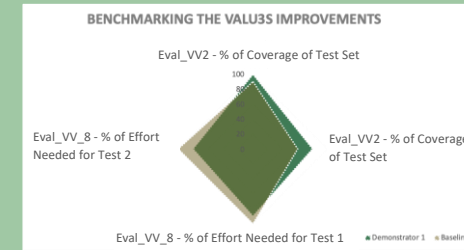
HW set up including a whole radar system producing a radar point cloud from the simulated scenario



The simulation of traffic scenarios enables forward integration of Tier 1 validation steps



## Improvement and Impact



Due to the lead demonstrator effort needed for testing, the cost of test equipment was reduced. Further, Former Tier 1 test scenarios were realised; thus, the development cycle of ADAS functions can be shortened, leading to a competitive advantage for customers.

### Participating partners





### 3.4 Use Case 4

## Demonstrators of Use Case 4

### - Human-Robot- Interaction in Semi- Automatic Assembly Processes



#### Use Case Description

UC4 is based on a Human-Robot-Interaction (HRI) process on the shop floor of a manufacturing-like environment. The process itself involves the execution of assembly tasks by human workers, focusing on the assembly of transformer units which consist of multiple parts.



#### Challenges addressed by the lead demonstrators

- Virtual validation and testing of the fault tolerance of an architecture design.
- Enhancing failure detection by Machine Learning techniques to identify faults in manipulated data streams.

#### Demonstrations

- 1) Handling and Gripping of Products / Parts (Lead)
- 2) ML-Pipeline (Lead)
- 3) Virtual & augmented reality-based user interaction V&V (Complementary)

#### UC in the web repository



## Handling and Gripping of Products / Parts

The demonstrator is based on a Human-Robot-Interaction (HRI) process on the shop floor of a manufacturing-like environment. The process itself involves the execution of assembly tasks by human workers, focusing on the assembly of transformer units which consist of multiple parts.

The demonstrator consists of the following two test cases that focus on the involvement of a human worker:

“Remove the product from simulation” (failure simulation) – (robot should stop immediately) and “Do not grip in a simulation” (failure simulation)

### Link to demo pitch video

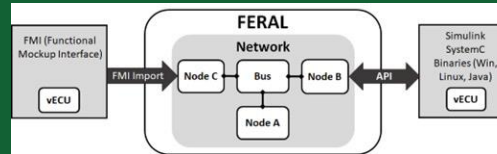


### Contact person for the demo

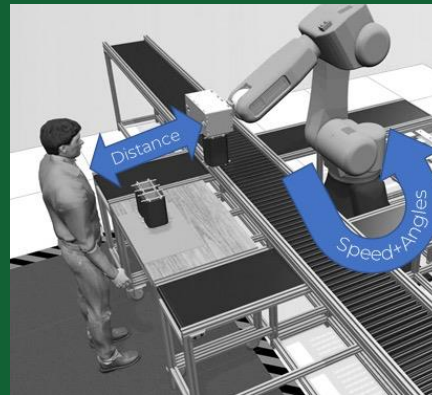
Iron Prandoda Silva  
(Iron.PrandodaSilva@iese.fraunhofer.de)

## Impressions

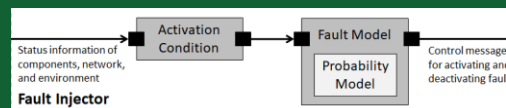
Coupling of different types of simulation models into a holistic simulation scenario



The validation object is a virtual model of the distributed production facility, which contains dedicated virtual models for the production line parts, sensors, and communication networks integrated into a holistic simulation scenario



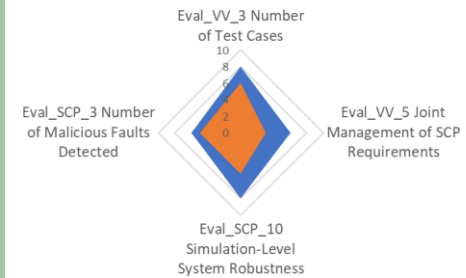
Fault injection component with its parts and internal flow of data and messages



## Improvement and Impact

### Benchmarking the VALU3S Improvements

■ Demonstrator UC4 Gripping Scenarios ■ Baseline UC4 Gripping Scenarios



Several functional and non-functional requirements (resp., fault tolerance and robustness) can be checked using dedicated simulation models and fault injection. Extending the fault model can increase the detection rate of additional fault types.

### Participating partners



## ML-Pipeline

The ML-Pipeline enhances failure detection by Machine Learning techniques by analysing real data and manipulating data streams in order to detect anomalies in the to-be process. This will be achieved through process mining and pattern recognition in data from the original assembly process used to develop and train a dedicated ML model.

### Link to demo pitch video



### Contact person for the demo

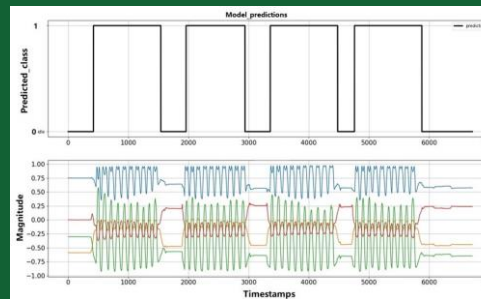
Zain Shahwar  
(zain.shahwar@pumacy.de)

## Impressions

Closed loop fault detection and diagnosis framework in virtual semi-automated assembly process. The simulation framework FERAL enables the coupling of the different involved tools and the integration and execution of the complex test scenarios.

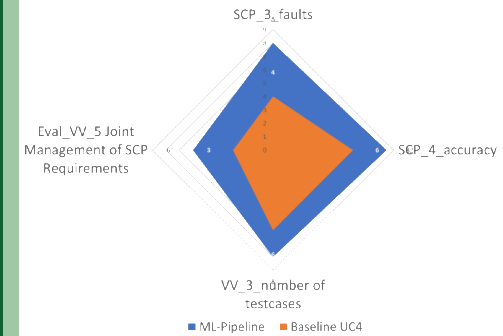


Activity recognition by using Long Term Short Memory (LSTM) networks is well-suited to learn from experience to classify, process and predict time series events when there are very long-time lags of unknown size between important events.



## Improvement and Impact

### Benchmarking the VALU3S Improvements



A model's accuracy depends on the available data's quality and volume. Both increase over time and help to train and improve the model to detect additional faults and events.

### Participating partners



### Virtual & augmented reality-based user interaction V&V

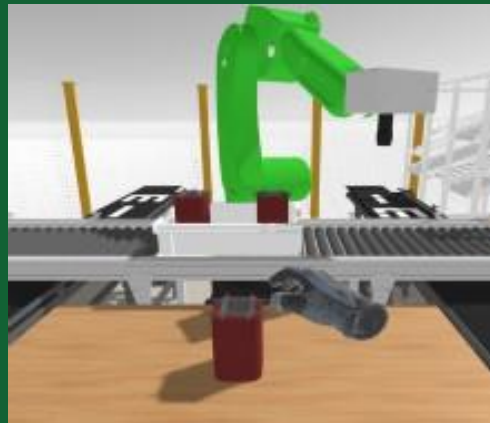
An immersive virtual reality application, namely XR-4-V&V, has been developed to facilitate early human-robot collaboration. This system allows human workers to collaborate with industrial robots in a simulated environment through the use of a head-mounted display. XR-4-V&V is developed using the Unity3D platform and focuses on handling only human interaction. Meanwhile, the robot simulation model runs on the CIROS studio, and the communication between the two is facilitated by FERAL, utilizing MQTT for message exchange.

### Contact person for the demo

Arturo Simon Garcia  
(ArturoSimon.Garcia@uclm.es)

### Impressions

3D representation of the working environment, consisting of the robot, that is carrying out the transformer assembly tasks and how the worker is acting (hand) which can be monitored throughout the process to analyse human factors and technology uptake.



### Improvement and Impact

To improve realism, the XR-4-V&V provides a 3D representation of the working environment, including the robot, which enables the execution of assembly tasks for transformer units considered for this use case. The human worker can observe the robot's movements while it grips the transformer parts. After the robot completes its task, the human worker can assemble the parts and wait for the robot to retrieve them. Throughout the entire process, the human operator's behavior can be monitored, enabling the analysis of human factors and technology acceptance before the system's full deployment.

### Participating partners



### 3.5 Use Case 5

## Demonstrators of Use Case 5

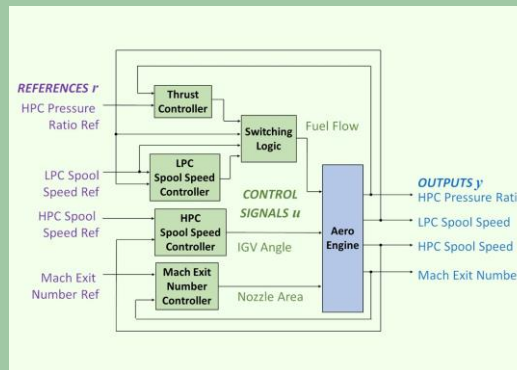
-

## Aircraft Engine Controller



### Use Case Description

UC5 focuses on V&V of an aircraft engine (linear model) and associated controllers. In order to demonstrate resilience to sensor faults, a voting mechanism is also integrated with the system model.



### Challenges addressed by the lead demonstrators

- Reducing requirement formalisation effort (through refactoring)
- Increasing testing coverage (through symbolic and interval methods)
- Reducing testing effort (in execution time and number of test cases)

### Demonstrations

- 1) Model based Design and Validation of the Hybrid Model (Lead)
- 2) Mu-FRET: Verifying & Refactoring Formalised Requirements (Lead)
- 3) Pre-Injection Analysis for Model-Implemented Fault- and Attack Injection (Lead)
- 4) SimuLation-based Verification (SiLVer) Workflow & Tool (Lead)

### UC in the web repository



## Model based Design and Validation of the Hybrid Model

The demonstrator aims to obtain certified proof of the stability of hybrid systems using symbolic techniques. The evaluation focuses on two aspects: synthesising a robust region (with fixed reference values) and robustness to reference value changes.

Link to demo pitch video



Contact person for the demo

Ludovico Battista  
(lbattista@fbk.eu)

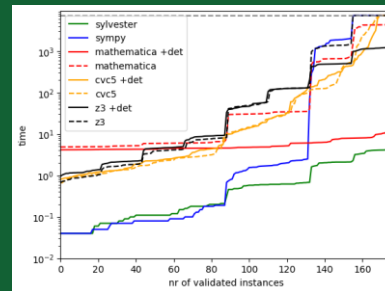
## Impressions

We approach these two targets by use of the tool Sabbath, that is integrated into an ad-hoc script.

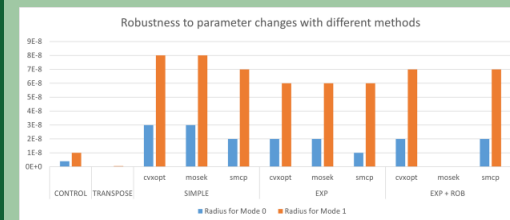
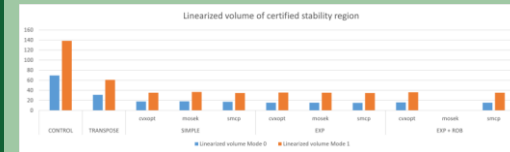
```

Valu3a_demo>python3 verify_po.py --solver z3 --use-exponential --size 5
>> Read matrices
A size 5x5
B size 5x22
C size 4x5
>> Controller matrices
KP1 size 3x4
KP2 size 3x4
KI1 size 3x4
KI2 size 3x4
INFO: main:Reference values: [1/2, 5.0, -1.0, 20.0]
INFO: main:Finding assumptions...
INFO: main:Searching a lyapunov function candidate...
CRITICAL:root:Synthesizing lyapunov with exponential
CRITICAL:root:Found alpha = 4.19
CRITICAL:root:Solving with cvxopt
    
```

The results obtained by comparing these methods are presented in the table. The figure represents the number of validated instances over time by the symbolic methods.



## Improvement and Impact



The quantitative improvement can vary based on how many test cases belong to the synthesised region of certified stability. Therefore, the total saving depends on the density of the test cases.

## Participating partners



## Mu-FRET: Verifying & Refactoring Formalised Requirements

Mu-FRET extends FRET, a framework for the elicitation, specification, formalisation and understanding of requirements, by adding refactoring functionality for formalised requirements.

Mu-FRET enables a user to extract parts of a requirement to a new requirement, allowing the extracted part to be reused. Mu-FRET also formally verifies that the refactored requirement (including the extracted parts) has the same behaviour as the original requirement.

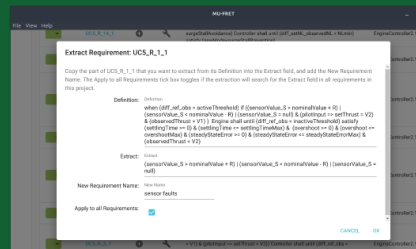
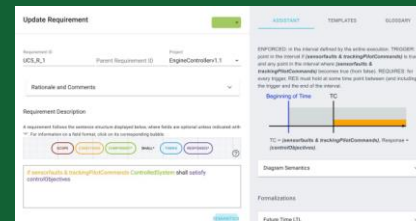
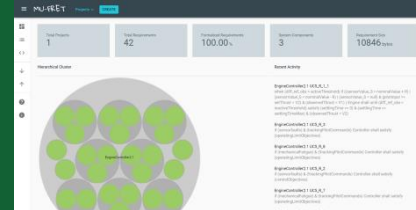
**Link to demo pitch video**



**Contact person for the demo**  
 Rosemary Monahan  
 (Rosemary.Monahan@mu.ie)

## Impressions

Snapshots from refactoring in the Mu-FRET tool



Mu-FRET on Github



## Improvement and Impact

Refactoring Requirements			
ID	Fragment Name	of (Re)Definitions	
		Before Refactoring	After Refactoring
F1	Sensor Faults	8	1
F2	Tracking Pilot Commands	13	1
F3	Control Objectives	18	1
F4	Regulation Of Nominal Operation	14	1
F5	Operating Limit Objectives	6	1
F6	Mechanical Fatigue	8	1
F7	Low Probability Hazardous Events	8	1
F8	Active	28	1
F9	Not Active	28	1
<b>Total (Re)Definitions</b>		132	9

**Formalising Requirements in UC5:**  
 Natural language requirements: 14  
 Original Test Cases: 20  
 Formalised requirements: 42

**Impact:** Demonstrated significant ambiguities present in the natural-language requirements that were identified and captured by formalising the requirements, thus reducing the number of potential safety/security requirement violations (Eval\_SCP2)

## Participating partners



**Maynooth University**  
 National University of Ireland Maynooth



## Pre-Injection Analysis for Model-Implemented Fault- and Attack Injection

Improvements obtained with pre-injection analysis for model-implemented fault- and attack injection are demonstrated.

Pre-injection analysis is used for reducing the error space to improve the efficiency of the injections. *Inject-on-read*, *inject-on-write* and *error space pruning of signals* pre-injection analyses are applied on a Simulink model of the UC5 aero engine controller using the MODIFI tool.

### Link to demo pitch video

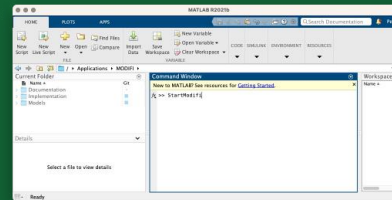


### Contact person for the demo

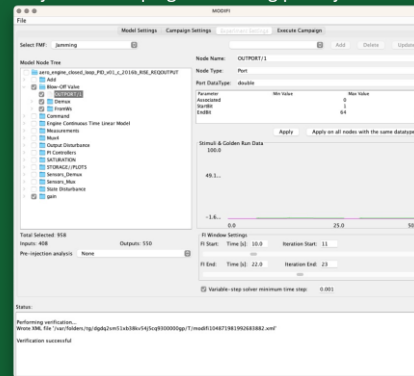
Peter Folkesson  
(peter.folkesson@ri.se)

## Impressions

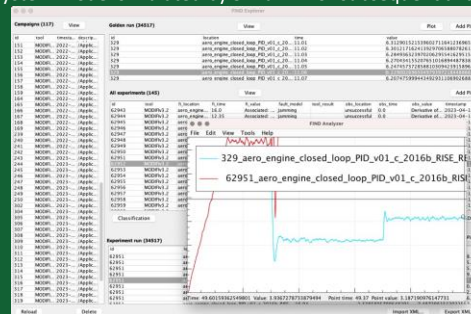
MODIFI is started from the MATLAB command window.



The MODIFI GUI allows configuration and execution of fault/attack injection campaigns including pre-injection analyses.

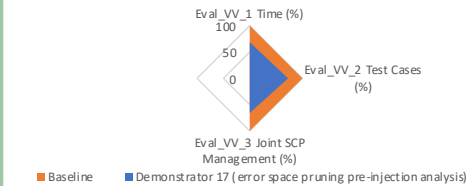


MODIFI monitors and stores selected signals of the target system model simulated by Simulink for subsequent analysis.



## Improvement and Impact

### Benchmarking the VALUS Improvements



The diagram above shows the improvements, in terms of reduced test execution time and a number of test cases, for error space pruning of signals pre-injection analysis applied on UC5. Joint management of safety, cybersecurity and privacy is also improved since both safety and cybersecurity requirements may be verified jointly when injecting fault- or attack models considered equivalent. These improvements are expected to reduce the time and cost of performing injection-based V&V.

### Participating partners





## SimuLation-based Verification (SiLVer) Workflow & Tool

The developed workflow aims to be a near-drop-in replacement for the Monte Carlo simulation, providing better coverage (through interval analysis) and, at the same time, reduced test execution time. Using C++ code as the analysis target enables the application of the process throughout the system design cycle. Templates are provided to ease the translation of requirements and system models.

**Contact person for the demo**  
 Georgios Giantamidis  
 (georgios.giantamidis@collins.com)

## Impressions

SiLVer main configuration YAML file – points to other configuration / input files and contains analysis options

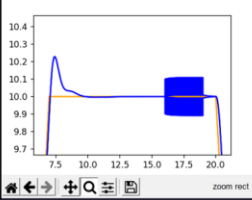
```

1 system: system.yaml
2 input-scenarios: input.yaml
3 output-dir: output
4
5 simulation:
6   enabled: yes
7   type: verification
8   # falsification -> typical simulation using floating point quantities
9   # verification -> reachability analysis using affine arithmetic
10
11 monitoring:
12   enabled: yes
13   type: 2
14   # 1 -> detect changes in reference and measure
15   # quantities of interest in output
16   # 2 -> use uncertainty ranges from input and
17   # measure quantities of interest in output
18
19 # desired bounds on measured quantities
20 # for requirement satisfaction
21 overshoot: 0.1
22 settling-time: 4
23 steady-state-error: 0.01
24
25 signals: # what should be monitored
26   reference: r(s)
27   output: y(s)
28
29 plotting:
30   enabled: yes
31
32 signals: [ # each row corresponds to a separate a plot
33   [r(1), y(1)],
34   [r(2), y(2)],
35   [r(3), y(3)]
36 ]
    
```

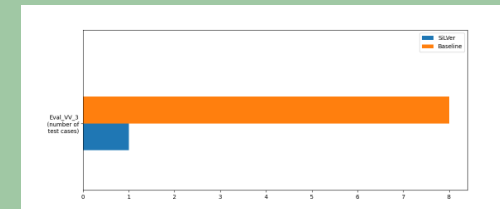
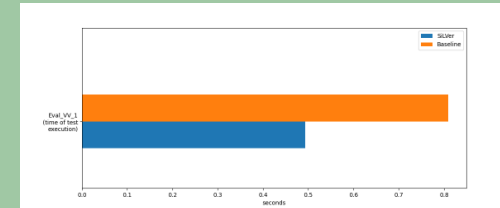
SiLVer output example – includes information about requirement satisfaction and system trajectory plots

```

t: 15.998
t: 17.998
t: 19.998
t: 21.998
t: 23.998
t: 25.998
t: 27.998
t: 29.998
t: 31.998
t: 33.998
t: 35.998
t: 37.998
t: 39.998
done!
elapsed time: 23.954 seconds
generating monitor code...
compiling...
g++ -std=c++11 -O3 reqmon2_generated.cpp -o m.exe
running monitor...
start: 15.998
stop: 19.498
settling time: 1.736 (req. satisfied)
overshoot: 1.06178 % (req. satisfied)
steady state error: 0.0621884 % (req. satisfied)
plotting...
    
```



## Improvement and Impact



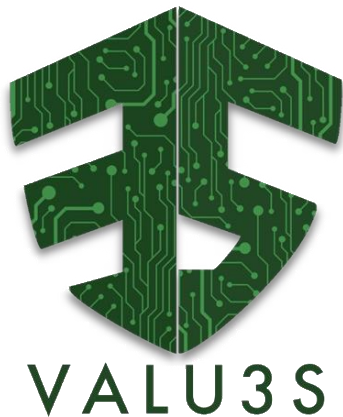
- Improved test execution time and reduced number of test cases
- Improved V&V automation & applicability
- Reduced overall certification effort

## Participating partners



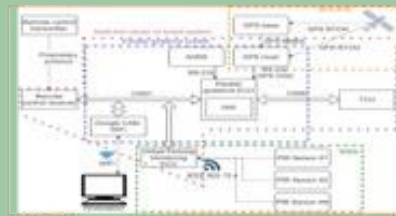
## 3.6 Use Case 6

## Demonstrators of Use Case 6 - Agricultural Robot



### Use Case Description

The target is integrating an autonomous guidance system, developed with safety and cybersecurity awareness, in an already existing multi-utility machine for agriculture and forestry.



### Challenges addressed by the lead demonstrators

- To define and address safety-critical aspects in a new application field in compliance with standards related to using robots and automated systems in agriculture.

### Demonstrations

1. MSA-FLA with CHESS-FLA (Lead)
2. Arm Unity (Lead)
3. Risk analysis with RAMSES tool (Complementary)
4. IEE 802.15.4 wireless sensor network – Intrusion Detection (Complementary)
5. Data-driven Fault Detector (Complementary)
6. Machine learning methods based on rules (Complementary)
7. Radio-link security of agricultural robot (Complementary)

### UC in the web repository



## MSA-FLA with CHES-FLA

Demonstration of applying the Model-based Safety Analysis with Failure Logical Analysis (MSA-FLA) method supported by the CHES-FLA tool. Starting from the designed functional model of the systems, we will show how to enrich this model with the failure behaviour description of each system subcomponent, how to apply the Failure Logical Analysis, and to automatically compute the FMEA (Failure Mode and Effect Analysis) table and the FTs (Fault Trees).

### Link to demo pitch video

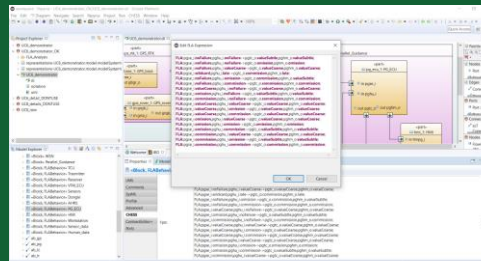


### Contact person for the demo

Katia Di Blasio  
(katia.diblasio@intecs.it)

## Impressions

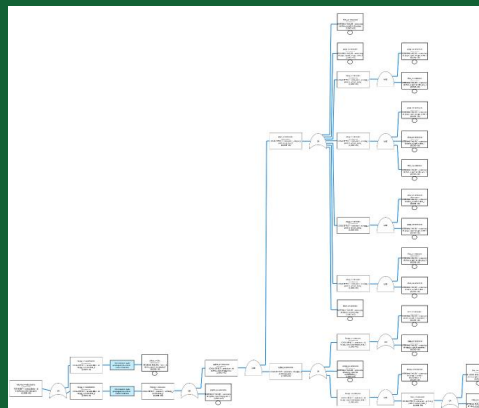
Screen of the CHES tool with a highlight of the FLA rules of a specific sub-block



Some FMEA rows automatically generated by the CHES-FLA tool

SYSTEM PATH	FUNCTION	FAILURE MODES	LOCAL EFFECTS	END EFFECTS	COMPENSATING PROVISION	SEVERITY	SAFETY EXPERT	FAILURE RATE
Agri_bot_interface... FailureMode_1	Control_1	(Status_1)notFailure	LATE failure at status_1	Agri_bot_movement.on				
Agri_bot_interface... FailureMode_1	Control_1	(Status_1)notFailure	LATE failure at status_1	Agri_bot_movement.off				
Agri_bot_interface... FailureMode_1	Control_1	(Status_1)notFailure	VALUACCURSE failure	Agri_bot_movement.on				
Agri_bot_interface... FailureMode_1	Control_1	(Status_1)notFailure	VALUACCURSE failure	Agri_bot_movement.off				
Agri_bot_interface... FailureMode_1	Control_1	(Status_1)omission	OMISSIO failure at status_1	Agri_bot_movement.on				
Agri_bot_interface... FailureMode_1	Control_1	(Status_1)omission	OMISSIO failure at status_1	Agri_bot_movement.off				
Agri_bot_interface... FailureMode_1	Control_1	(Status_1)omission	OMISSIO failure at status_1	Agri_bot_movement.on				
Agri_bot_interface... FailureMode_1	Control_1	(Status_1)omission	OMISSIO failure at status_1	Agri_bot_movement.off				

One of the FT automatically generated by CHES-FLA



## Improvement and Impact

The Model-based Safety Analysis with Failure Logical Analysis (MSA-FLA) performed with the CHES-FLA tool allowed obtain the following quantitative results:

- 10 different consequences of not detecting the disconnection from the remote controller have been analysed.
- 10 different consequences of not detecting the disconnection from the IMU have been analysed.
- Reduction of the time needed to perform a Hazard Analysis and Risk Assessment by a factor of 0.6.

### Participating partners



### Arm Unity

Software component testing using an open-source SW framework adapted during the VALU3S project to be executed directly on the target device instead of being executed on a PC.

Arm Unity tool integrates the SW component testing framework and the semi-hosting feature of the serial wired debug interface to execute the tests on the target device and collect the test result on the PC.

#### Link to demo pitch video

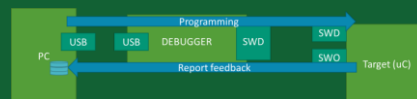


#### Contact person for the demo

Emanuele Mingozi  
(mingozzi@estetechnology.com)

### Impressions

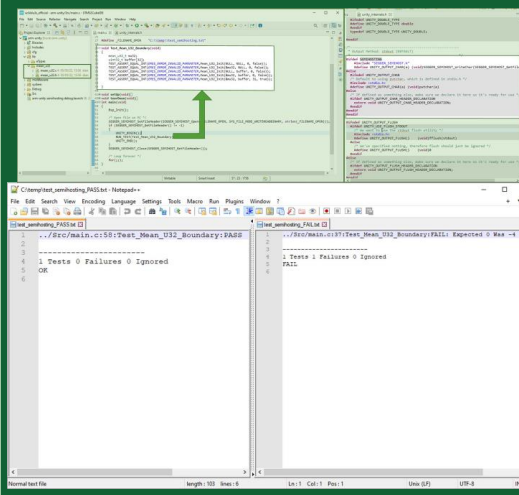
Block diagram of Arm Unity configuration



Test-bench based on Arm Unity



Arm Unity usage and test reports



### Improvement and Impact

The advantages are to compile and execute the code directly on the target device. The automotive and agricultural standards ISO 26262 and ISO 25119 have in the verification and validation process both the SW tests and the HW/SW integration test step.

With the Arm Unity tool, it is possible to execute both the test steps in a single step, reducing from 5% to 10% the effort needed for SW component and HW/SW integration tests, thanks to less testbench to be prepared and less code modification required to perform the component testing directly on the device under test.

#### Participating partners



## RAMSES tool for Risk Management of Agriculture Robot

Using the RAMSES tool, the Risk Management Process of Agriculture robot considered in UC6 is undertaken. The Risk management process implemented within RAMSES follows prescriptions of ISO12100.

The digital tool allows to create and assess risk scores of hazardous scenarios related to the operations of the agriculture robot. Furthermore, following ISO standards, safety measures can be added to mitigate the risk score of each scenario when necessary.

### Link to demo pitch video



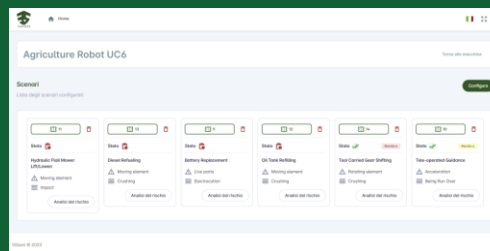
### Contact person for the demo

Davide Ottonello  
(d.ottonello@stamtech.com)

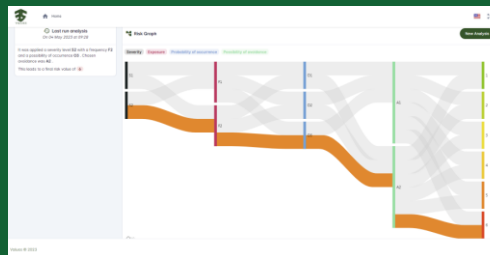
## Impressions

Demonstrator shows how, thanks to RAMSES digital tool, risk management process can be performed in a faster and easier way while being compliant with ISO12100 standard and related safety prescriptions.

The safety engineer can easily create a set of hazardous scenarios referencing list of hazards contained in ISO12100.



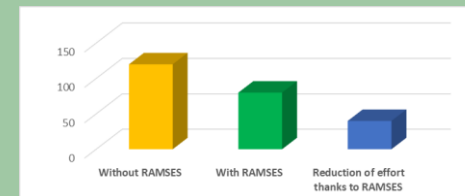
Each scenario can then be evaluated through risk graph methodology to obtain the overall risk score. Last, safety measures can be added to lower the risk score of the scenario at least by one, as the standard prescribes.



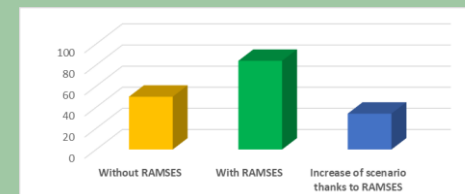
## Improvement and Impact

The introduction of RAMSES tool into a state-of-the-art risk management process applied in the use case has led to two major benefits:

- The man-hours needed to conduct the overall risk analysis has been reduced from 120 to 80, i.e. -33%



- The number of hazards considered has been increased from 50 to 84 (on average), i.e. + 68%



### Participating partners





### 3.7 Use Case 7

## Demonstrator of Use Case 7 - Human-Robot Collaboration in a Disassembly Process with Workers with Disabilities



### Use Case Description

**Use Case 7** targets a collaborative robotic cell to remove refrigerator magnetic gaskets in a human-robot interaction context. The system applies machine learning techniques for grasping and removing the gasket.



### Challenges addressed by the lead demonstrators

- Verification and validation of the complete system in a safe test environment identical to the actual disassembly plant.
- Reducing personnel cost as no human-in-the-loop is required.
- Multiple test batches generated to verify and validate the generalization capability of reinforcement learning agents.

### Demonstration

- 1) Coordination of test generation and validation in simulation-based human-robot collaborative environments (HuRoCTest)

UC in the web repository



### Coordination of test generation and validation in simulation-based human-robot collaborative environments (HuRoCTest)

The **lead demonstrator** of UC7 coordinates simulation-based testing activity in human-robot interaction environments. The HuRoCTest tool provides a real-time, automated verdict of test execution of simulation environments through constrained-based-oracles using simulation-based testing for human-robot interaction. To coordinate the testing with the constrained-based oracle, it leverages a ROS package to seamlessly align the execution of the test, the simulation environment, and the oracle.

#### Link to demo pitch video



#### Contact person for the demo

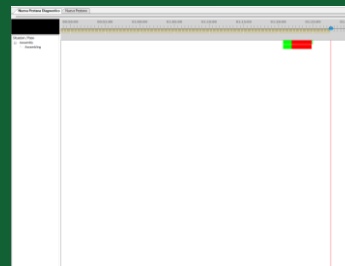
Joseba A. Agirre  
(jaagirre@mondragon.edu)

### Impressions

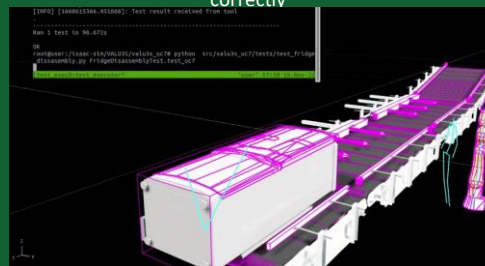
**NVIDIA Isaac Sim.** Simulation environment for the validation of the human-robot interaction robotic system.



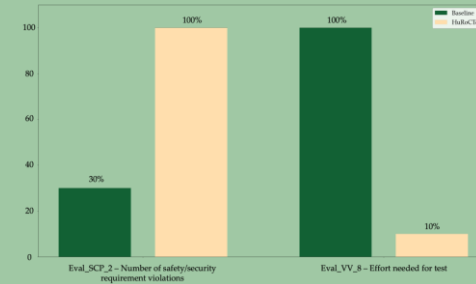
**ULISES.** Procedural-task evaluation approach for testing simulation-based human-robot interaction.



**HuRoCTest.** ULISES receives the topics from ROS system and uses constraint-based rules to determine whether the robot performs the disassembly correctly



### Improvement and Impact



As a result of the lead demonstrator, a more extensive range of tests could be conducted that not only assessed the safety of the reinforcement learning agent but also encompassed the safety of the entire disassembly plant. Furthermore, all of these tests were automated, thus removing the requirement for human intervention in the testing process, potentially reducing personnel expenses related to testing tasks.

#### Participating partners



### 3.8 Use Case 8

## Demonstrators of Use Case 8

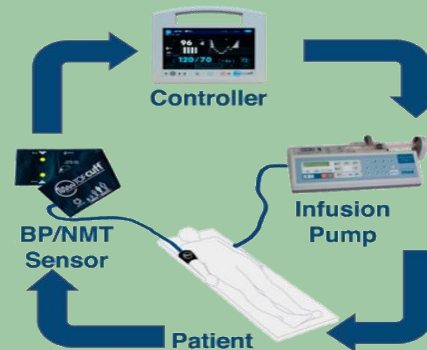
### NMT Infusion Controller



#### Use Case Description

An NMT (NeuroMuscular Transmission) Infusion controller maintains the patient's muscle relaxation under target during an O.R. operation. This UC8 is about the testbench platform developed to optimise the control algorithm.

#### Physiological control



#### Challenges addressed by the lead demonstrators

Avoid experimental and clinical testing until the system has been thoroughly tested under laboratory conditions, thus reducing costs and shortening development time

#### Demonstrations

- 1) **NMT Simulator:** TestBench Platform for NMT controller
- 2) **MSA-FLA with CHES-FLA:** Model-based Safety Analysis with Failure Logical Analysis
- 3) **Early V&V in Knowledge-Centric Systems Engineering:** Specification quality analysis and Traceability management

#### UC in the web repository





## NMT simulator

This demonstrator is a Testbench platform that can support defining the algorithm that provides the best performance in NMT (NeuroMuscular Transmission) control. It makes use of a Patient's Model that responds to the patient (in NMT units) to a given dose infusion during the control period.

### Link to demo pitch video

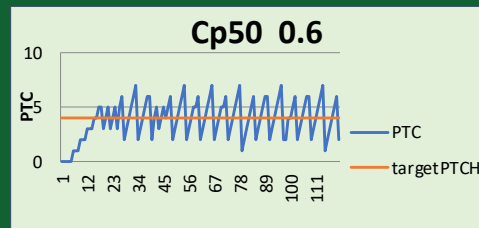


### Contact person for the demo

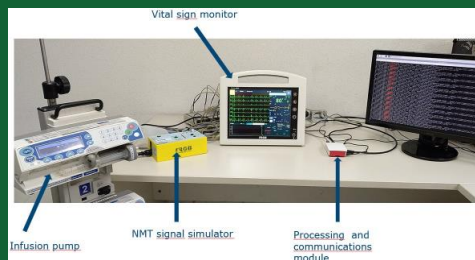
Ricardo Ruiz  
(rruiz@rgb-medical.com)

## Impressions

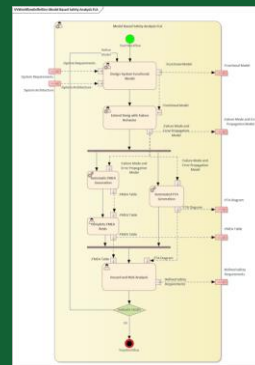
Screen of the NMT Controller results under specific testing conditions.



### NMT simulation tool



### Workflow definition



## Improvement and Impact

In order to verify the correct behaviour of the NMT simulator, the simulator can be run with different patient configurations. The following quantitative results have been obtained:

- 90% cost reduction is obtained by making it possible to operate at the laboratory level in the first stage of development. The time needed to analyse the performance of different potential strategies has been reduced.
- Up to 5 potential hazard situations deriving from the erroneous behaviour of the Controller have been identified.
- More than 10 different patient characteristics that could affect the performance of the Controller can be analysed.

### Participating partners



### MSA-FLA with CHES-FLA

Demonstration of the application of the Model-based Safety Analysis with Failure Logical Analysis (MSA-FLA) method supported by the CHES-FLA tool. Starting from the designed functional model of the systems, we will show how to enrich this model with the failure behaviour description of each system subcomponent, how to apply the Failure Logical Analysis and to automatically compute the FMEA (Failure Mode and Effect Analysis) table and the FTs (Fault Trees).

**Link to demo pitch video**

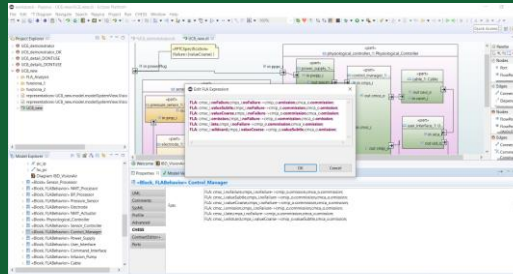


**Contact person for the demo**

Katia Di Blasio  
(katia.diblasio@intecs.it)

### Impressions

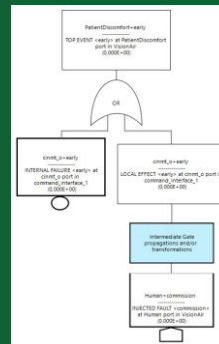
Screen of the CHES tool with a highlight of the FLA rules of a specific sub-block



Some FMEA rows automatically generated by the CHES-FLA tool

SYSTEM PATH	FUNCTION	FAILURE MODES	LOCAL EFFECTS	END EFFECTS
VisioAnkri.physiological_controller_Controller_manager_3	Control	Control_failure	OMISSION failure at omip_p_port	VisioAnkri.gpdiagnostic.omiission
VisioAnkri.physiological_controller_Controller_manager_3	Control	Control_failure	OMISSION failure at omip_p_port	VisioAnkri.gpdiagnostic.valueState
VisioAnkri.physiological_controller_Controller_manager_3	Control	Control_failure	OMISSION failure at omip_p_port	VisioAnkri.gpdiagnostic.valueState
VisioAnkri.physiological_controller_Controller_manager_3	Control	Control_failure	OMISSION failure at omip_p_port	VisioAnkri.gpdiagnostic.commission

One of the FT automatically generated by CHES-FLA



### Improvement and Impact

The Model-based Safety Analysis with Failure Logical Analysis (MSA-FLA) performed with the CHES-FLA tool allowed obtain the following quantitative results:

- 9 potential hazard situations deriving from the erroneous behaviour of the Controller have been identified.
- 72 sequences or combinations of events that may cause a hazardous situation have been identified.
- The time needed to analyse the performance of different potential strategies has been reduced by a factor of 0.6.
- 6 different characteristics that could affect the safety of the Controller have been analysed.

**Participating partners**



## Early V&V in Knowledge-Centric Systems Engineering

Two KCSE methods have been improved in VALU3S for early V&V: (1) Compliance-Aware Extended Knowledge-Centric System Artefact Quality Analysis and (2) Extended Knowledge-Centric Traceability Management. The methods and their supporting tools have been applied to UC8 data:

- Risks analysis
- System models
- Applicable standards

### Link to demo pitch video



### Contact person for the demo

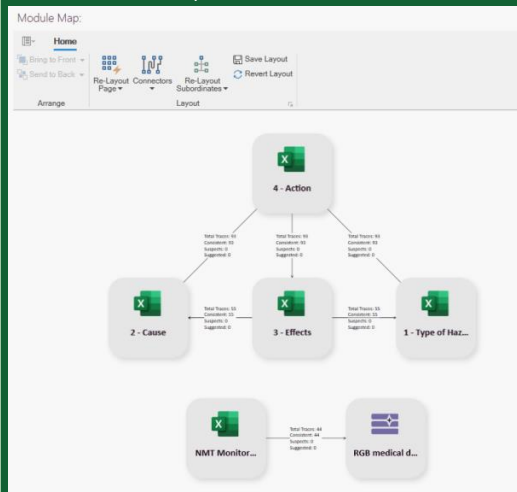
Jose Luis de la Vara  
(JoseLuis.deLaVara@uclm.es)

## Impressions

RQA tool screenshot

Consistency	Completeness	Similar requirements	Correctness	Value	Summary	Mandatory	Weight
✓	✓	✓	★ ★ ★	1	Avoid the use of indefinite Articles	<input type="checkbox"/>	1
✓	✓	✓	★ ★ ★	1	Avoid the use of Passive Voice out of...	<input type="checkbox"/>	1
✓	✓	✓	★ ★ ★	1	Missing quantifier (Measurement unit or noun)	<input type="checkbox"/>	1
✓	✓	✓	★ ★ ★	1	Avoid misspelling	<input type="checkbox"/>	1
✓	✓	✓	★ ★ ★	2	Long requirements (measured in paragraphs) must be...	<input type="checkbox"/>	1
✓	✓	✓	★ ★ ★	0	N/A	<input type="checkbox"/>	1
✓	✓	✓	★ ★ ★	0	N/A	<input type="checkbox"/>	1
✓	✓	✓	★ ★ ★	0	N/A	<input type="checkbox"/>	1
✓	✓	✓	★ ★ ★	0	N/A	<input type="checkbox"/>	1
✓	✓	✓	★ ★ ★	0	N/A	<input type="checkbox"/>	1
✓	✓	✓	★ ★ ★	0	N/A	<input type="checkbox"/>	1
✓	✓	✓	★ ★ ★	0	N/A	<input type="checkbox"/>	1
✓	✓	✓	★ ★ ★	0	N/A	<input type="checkbox"/>	1
✓	✓	✓	★ ★ ★	0	N/A	<input type="checkbox"/>	1
✓	✓	✓	★ ★ ★	0	N/A	<input type="checkbox"/>	1
✓	✓	✓	★ ★ ★	0	N/A	<input type="checkbox"/>	1

Traceability Studio tool screenshot



## Improvement and Impact

Wider system artefact quality analysis

- Tens of new analyses have been enabled, e.g., for system design models

More precise traceability management

- Trace specification, discovery and verification have been enhanced for hundreds of system artefact traces

Better system artefacts

- The quality of tens of system specification items has been increased

Lower effort in the addressed V&V tasks thanks to automated support

- 20-40% faster V&V

Lower cost in issue resolution thanks to early issue detection

- ~25% cost reduction

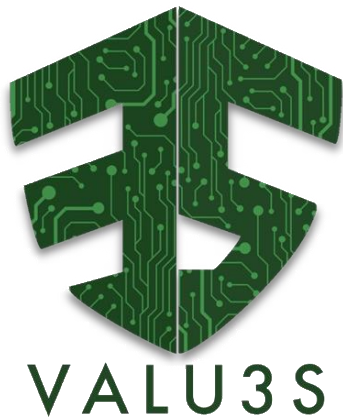
### Participating partners





### 3.9 Use Case 9

## Demonstrators of Use Case 9 - Autonomous Train Operations



### Use Case Description

Autonomous Train Operations is focused on validating Polaris, a Computer Vision System for signs and signals detection in the railway domain.

The validation process is carried out in a laboratory environment using synthetic data.



### Challenges addressed by the lead demonstrators

- Reduction of effort (time and cost) in the generation of dataset for system validation
- Evaluation of computer vision system's behavior in different operating conditions and detection of safety related issues

### Demonstrations

- 1) Validation of Computer Vision system using synthetic data generated

UC in the web repository



## Validation of Computer Vision system using synthetic data

The UC9 demonstrator comprises the validation process for a CV system trained using real images recorded in the field and validated using synthetic images. Using Train Simulator, a custom train journey is designed, and with the DaGe4V tool, frames in different light and weather conditions are recorded. VATRA executes the tests and analyses the results to get the system's metrics and provide test execution evidence.

### Link to demo pitch video



### Contact person for the demo

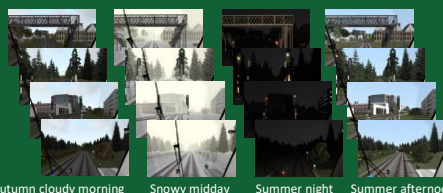
Xabier Mendialdua  
(xmendialdua@ikerlan.es)

## Impressions

Design of train journey using Train Simulator

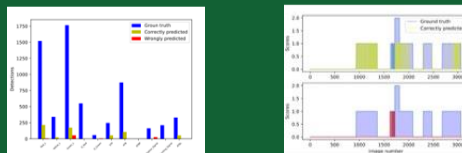


Generation of synthetic validation datasets using DaGe4V

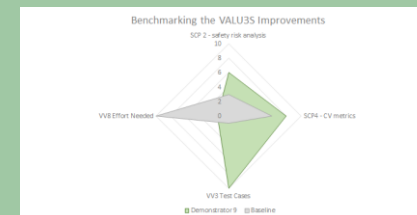


Autumn cloudy morning    Snowy midday    Summer night    Summer afternoon

Execution of validation tests and analysis of test results using VATRA to evaluate system's accuracy and detect safety related issues.



## Improvement and Impact



Validation process improvement impacts:

- the increase by a factor of 10 of the number of tests due to the automation of validation data generation.
- the diversity of operating conditions that can be tested thanks to using the simulator for data generation.
- the effort reduction by a factor of 25 by avoiding the need for field recordings.

### Participating partners

**ikerlan**  
MEMBER OF BASQUE RESEARCH  
& TECHNOLOGY ALLIANCE

**CAF** | SIGNALLING

### 3.10 Use Case 10

## Demonstrators of Use Case 10

-  
Safety function  
out-of-context



### Use Case Description

The platform to study and explore the new V&V methods with the collaboration of the interested partners is a SIL4 BLDC motor controller in the railway domain.

In railway signalling systems, the motor controller (e.g., used in point machines) receives safety function orders via a communication interface from the interlocking computer system (CIS) and acts upon these orders safely and on time. The motor controller has a deterministic state machine that defines its correct behaviour and failures.



### Challenges addressed by the lead demonstrators

Analysis of a minimal set of state-of-the-art Commercial off-the-shelf (COTS) components for SIL4 applications reached a maturity that can reduce the size, cost, and power consumption. Model-based testing using MoMuT produced tests that cover many behavioural faults. Also, verification and validation of the family of models of this controller were performed by UPPAAL and Uppex.

### Demonstrations

- 1) Safety verification and validation for the signalling railway application (Lead)
- 2) Implementing BLDC motor (Complementary)
- 3) Model checking with UPPAAL (Complementary)
- 4) MoMuT - Model based testing (Complementary)

### UC in the web repository



## Safety verification and validation for the signalling railway application

During the VALUS3 project, Alstom created a conceptual safety concept using a minimal set of state-of-the-art Commercial Off-The-Shelf (COTS) components for the signalling system in the railway domain. In this use case, we used this concept to develop a safety-critical motor object controller to verify and validate using Model Checking and Testing techniques.

- **The UPPAAL model checker** was used to verify the time-related properties of the software controller.
- **The Uppex tool** was used to configure variations of the UPPAAL model, increasing the applicability of the model.
- **The MoMuT toolset** was used to generate a minimal set of unit tests that cover a maximum number of changes to a simplified controller model.

Analysis of a minimal set of state-of-the-art COTS components for SIL4 applications reached a maturity that can reduce the size, cost, and power consumption.

### Link to demo pitch video

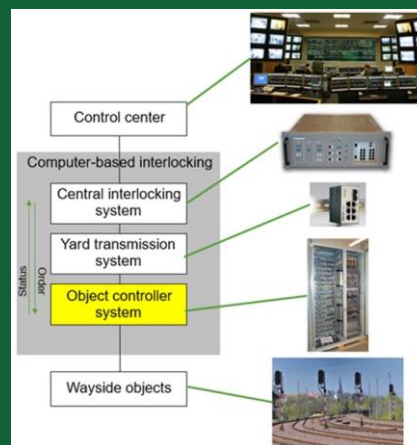


### Contact person for the demo

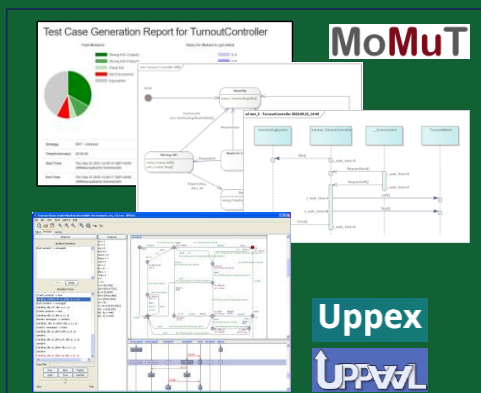
**Sina Borrami**  
 (sina.borrami@alstomgroup.com)  
**José Miguel Paiva Proença**  
 (pro@isep.ipp.pt)  
**Erwin Kristen**  
 (Erwin.Kristen@ait.ac.at)  
**Robert Sicher**  
 (Robert.Sicher@sparxsystems.eu)

## Impressions

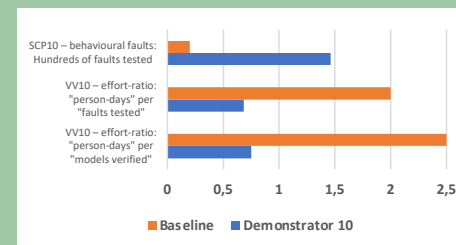
Architecture of the signalling railway system



Demonstrator Tool Framework



## Improvement and Impact



We measure both the effort required to create tests that cover behaviour models using MoMuT and the effort to formally verify properties using UPPAAL/Uppex. This effort is measured in person-days by keeping an estimate of how many people were involved and multiplying this value with the average accumulated time spent on these tasks. Furthermore, we consider the effort-per-result. I.e., we divide this effort in person-days by the number of results: the number of faults covered with MoMuT and the number of properties and variations of the formal model with UPPAAL/Uppex. We call this final number the "effort ratio" of our two formal methods. Note that more is worse, i.e., a larger effort ratio reflects a more significant time and cost per result, which is not desirable.

This demonstrator was evaluated with respect to the number of software faults that are tested (SCP10, where more is better), the effort (time \* person) for each fault tested (VV10, where less is better), and the effort for each property and model formally verified (VV10, where less is better).

### Participating partners



### 3.11 Use Case 11

# Demonstrators of Use Case 11

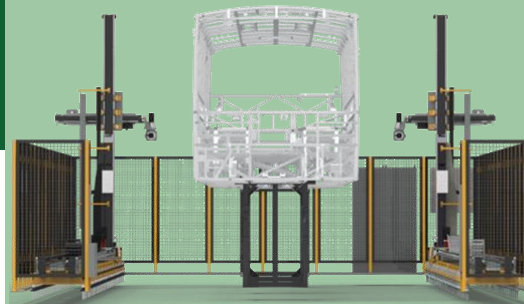
-

## V&V of an Automated Robot Inspection Cell for Automotive Body- in-White



### Use Case Description

UC11 focuses on a novel system using new AI and computer vision (AI/CV) techniques to shorten the quality check of the vehicles' parts through a more effective automotive body-in-white inspection. The baseline of this use case is to provide a better fault-tolerant production system to achieve better quality control.



### Challenges addressed by the lead demonstrators

- Automatic trajectory creation for each vehicle preventing collisions.
- Presence-absence check of 3000+ vehicle parts in less than 25 minutes of total inspection time
- Improve the cyber-physical safety and security in multistakeholder operations

### Demonstrated Innovations

1. Tailored Mutation-based Fault Injection Tool (IM-FIT)
2. Camera Fault Injection Tool (CamFITool)
3. Simulation-based Robot Verification Tool (SRVT)
4. Model-Aided Runtime Verification for Robotic Systems (MARVer)
5. PRIGM Randomness Test Suites, Vulnerability analysis of cryptographic system & hardware-based cyber resilience



### UC11 in the web repository





## Otokar Robot Inspection Cell for Automotive Body-in-white Simulation Tool

- ✓ This tool scans the CAD data of vehicles and determines which spaces are suitable for the physical movement of robots. Then, a robotic arm with a camera follows a safe trajectory to take snapshots and apply AI/CV to analyse the captured images.
- ✓ Pre-work interface to prevent software-related errors and accidents by creating a digital twin of robots in the field.
- ✓ Integrated with:
  - Safety trajectory planning with SRVT and IM-FIT.
  - CamFITool for sensor data manipulation check and anomaly detection
  - Integrated verification for safety and security of industrial robot inspection system with MARVer and vulnerability analysis with PRIGM

### Link to demo pitch video

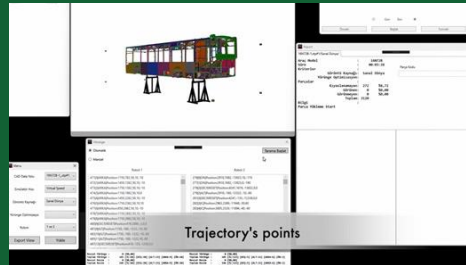


### Contact person for the demo

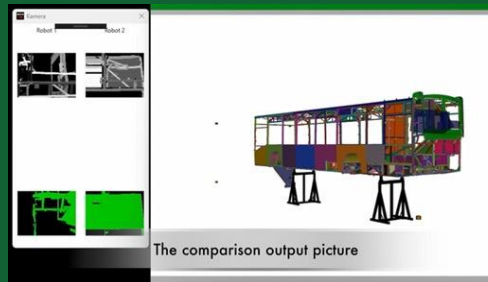
Gürol Çökünlü  
gcokunlu@otokar.com.tr

## Impressions

The software in the server side decides trajectory points, than robots start the part existence of vehicle in simulation environment



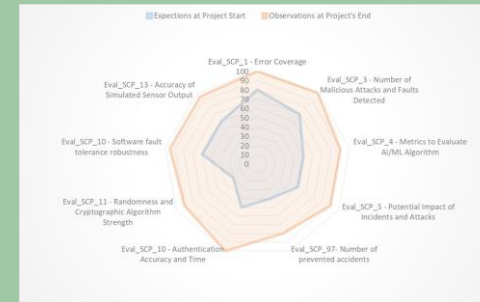
Virtual images which are taken by robots in simulation compares with CAD data of vehicle.



Finally, the quality inspection report is generated. We can see the seen parts,



## Improvement and Impact



### Coverage (%) of results adopted by the Industry (Otokar)

- State-of-the-art system in Safety, Cybersecurity, and Privacy.
- End-to-end secure integration of data in heterogeneous and multi-stakeholder networks.
- Better quality and control with less time and cost.
- 10 toolchains validated in 2 physical environments covering 10 main evaluation criteria and 30+ test cases
- Existence control of a minimum % of 95 parts of the vehicle in less than 25 minutes.

### Participating partners



### 3.12 Use Case 13

# Demonstrators of Use Case 13

-

## Industrial Drives for Motion Control



### Use Case Description

Industrial drives for motion control systems are often built with PLCs (Programmable Logic Controller) and power inverters for controlling electric motors and have many different application scenarios, such as factory automation and robotics.

The use case is built on a digital twin of such a system, which serves as a demonstration vehicle for the lead demonstrator with signal monitoring where specific simulation signals are verified against a formal specification with fault explanation.



### Challenges addressed by the lead demonstrators

A significant challenge is the verification of analogue signals interfaced to motor models. Their theoretically infinite state-space, together paired with non-linear behaviour, makes it hardly possible to verify every scenario—an easy-to-handle method for verifying signal behaviour, such as motor phase voltages, benefits verification activities.

### Demonstrations

- 1) Real-Time Analogue Signal Monitoring (RTAMT) for a Digital Twin for Motion Control (Lead)
- 2) Model-Based Mutation Test Modeling with Enterprise Architect for motor control (Complementary)
- 3) Processor Integration verification enabled by a digital twin (Complementary)

### UC in the web repository



## Real-Time Analogue Signal Monitoring for a Digital Twin for Motion Control

This demonstrator shows the use of the method "Fault Localization for Specification-based real-time monitoring" in the digital twin for motion control. The digital twin comprises a motor model modelled in the simulation tool AMESim, interfaced to virtual hardware peripherals implemented in SystemC, and a QEMU-based RISC-V model. The Real-time Analogue Monitoring Tool (RTAMT) is a runtime verification library, developed by AIT and is written in Python under the liberal BSD-3 license. RTAMT takes simulation measurements and requirements formalised in Signal Temporal Logic (STL) to evaluate a robustness degree, indicating how well the observed behaviour satisfies or how badly it violates the requirement. This demonstrator uses analogue signals, such as motor phase voltages from AMESim, to generate faulty simulation data. This data is then checked against the formally defined requirements. The graphical results generated by RTAMT help to identify fault areas quickly and increase verification quality.

### Link to demo pitch video

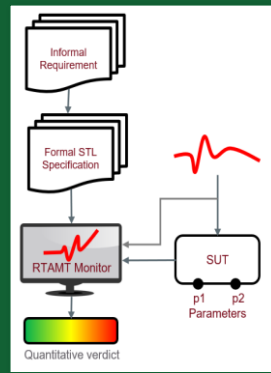


### Contact person for the demo

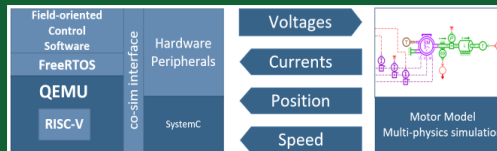
Bernhard Fischer  
[bernhard.bf.fischer@siemens.com](mailto:bernhard.bf.fischer@siemens.com)  
 Dejan Nickovic  
[dejan.nickovic@ait.ac.at](mailto:dejan.nickovic@ait.ac.at)

## Impressions

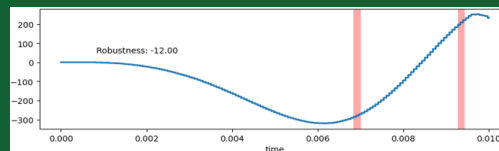
Flow with the Real-Time Analogue Monitoring Tool



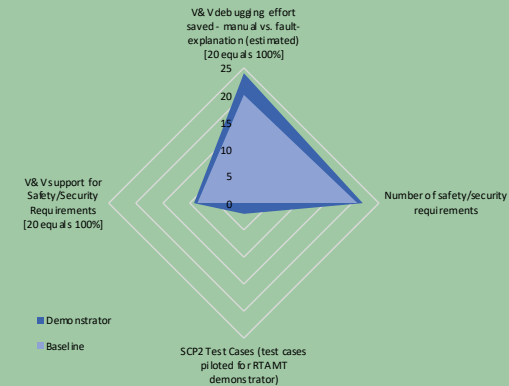
System-Under-Test (SUT): Motion Control Digital Twin built with AMESim, QEMU and SystemC



Example for RTAMT fault-explanation (specification violation) of motor phase voltage values



## Improvement and Impact



The V&V support with RTAMT for safety/security requirements was increased. The application of signal monitors can also increase the overall verification quality by revealing design flaws in the System-under-Test. Furthermore, signal monitoring also enables support for system optimisation (tighter/looser specification for signals) due to fault explanation and reduces debugging efforts by automatic monitor generation support.

### Participating partners



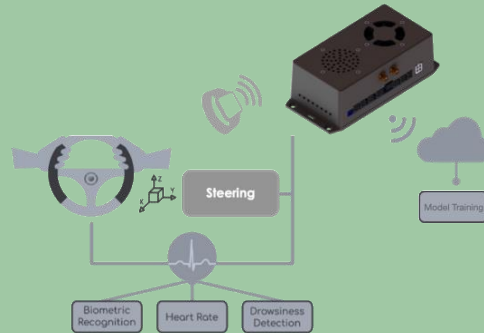
### 3.13 Use Case 14

# Demonstrators of Use Case 14 - CardioWheel



## Use Case Description

UC14 use case presents the CardioWheel as a critical system capable of driver monitoring and biometric identification as a rich environment for safety, cyber-security, and privacy validation & verification.



## Challenges addressed by the lead demonstrators

- Ensure a sound firmware architecture capable of handling all required tasks.
- Ensure robust cryptographic methods.
- Develop an objective metric for drowsiness.

## Demonstrations

- 1) Hardware-in-the-loop Validation Station.
- 2) Instrumented Driving Simulator for Drowsiness Data Generation

## UC in the web repository



## Hardware-in-the-Loop Validation Station

This demonstrator shows the result of combining runtime verification and fault injection methods into an automated full-system validation setup.

- Defines system requirements as formal statements verifiable by software monitors
- Implements software-based fault injection

### Link to demo pitch video



### Contact person for the demo

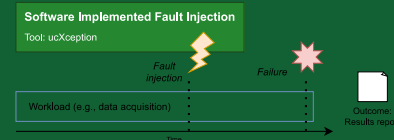
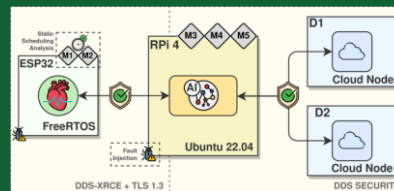
Lourenço Rodrigues  
(lar@cardio-id.com)

## Impressions

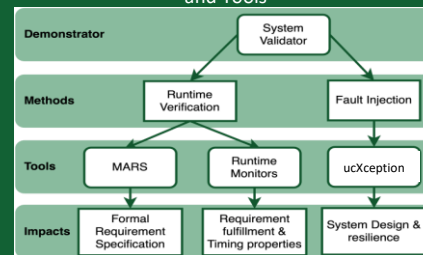
Validation Station with Touch Screen Simple Interface



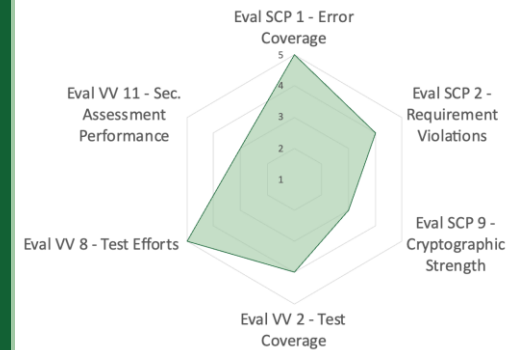
Monitor generation and fault injected are implemented as formal verification methods



Connection between Demonstrator and V&V Methods and Tools



## Improvement and Impact



Using the validation station, the validation process's duration decreased from 15 to 2 minutes per unit and liberated three qualified engineers from validation supervision, significantly reducing the costs.

### Participating partners



## Instrumented Driving Simulator for Drowsiness Data Generation

Two VTI's driving simulators were equipped with the CardioWheel to collect data, such as ECG, EOG, reaction time, and sleepiness score, from drowsy drivers. This activity is motivated by the fact that data quality and quantity are of the utmost importance to guarantee reliable predictions of machine learning systems based on human factors.

**Link to demo pitch video**



**Contact person for the demo**

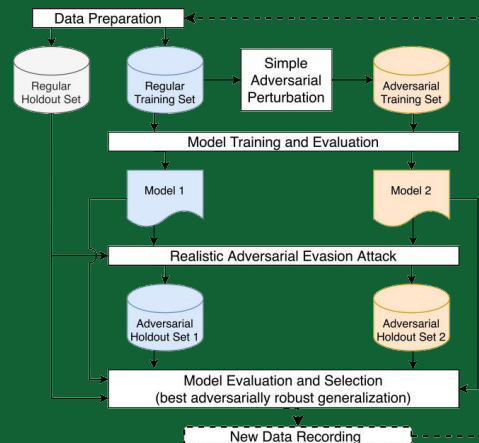
Maytheewat Aramrattana  
(maytheewat.aramrattana@vti.se)

## Impressions

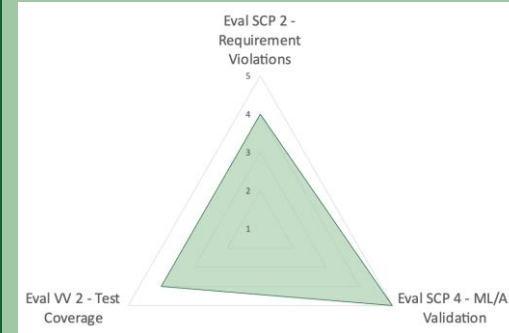
Driving simulator equipped with the CardioWheel to associate driver's drowsiness with their cardiac rhythm dynamics



Adversarial training method is used to increase model's robustness against noisy or faulty data



## Improvement and Impact



The demonstrator's efforts resulted in a new and rich drowsiness dataset that includes an objective drowsiness metric – reaction time, integrated in the simulators during the project's duration. An adversarial training procedure was tested on drowsiness data, demonstrating improved model robustness, with less than a 10% performance decrease for unknown drivers.

**Participating partners**





Thanks to all participants  
for the great project!





This 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.

Disclaimer: The ECSEL JU and the European Commission are not responsible for the content of this leaflet or any use that may be made of the information it contains.



## Chapter 4 Conclusion

The VALU3S project, funded by the European Union, has reached its culmination, marking the end of a journey that has been both challenging and rewarding. The project's primary goal was to lower the effort and cost of engineering processes by focusing on one (or more) of the most resource-consuming steps of the product life cycle – verification and validation (V&V) of autonomous systems, which was successfully achieved and demonstrated.

The demonstrations, aptly named "lead demos", synthesised the key project results. These demos were unveiled at the 9<sup>th</sup> consortium meeting in Vienna in May 2023 and will be showcased again at the final project event in Porto in June 2023. The Vienna event provided a compelling preview of the project's outcomes, and the Porto event is expected to offer a similar, even enhanced experience.

The project embraced a variety of formats to present its results, ranging from software and hardware demonstrations to leaflets, posters, and pitch videos. This multi-faceted approach ensured a comprehensive and engaging presentation of the project outcomes, enhancing the visitor experience and ensuring the project's results stayed in the minds of the audience.

The preparation and execution of the events were detailed in Chapter 2, while Chapter 3 focused on the best demonstrations of the Use Cases. All the lead demonstrators have been comprehensively presented in a leaflet, briefly summarising the project results. These publicly available leaflets will be distributed at the Porto event, further extending the project's reach.

Looking back, the "Final demo" is not only expected to reach its set goals but also provides a valuable platform for disseminating these significant achievements. The project team is immensely proud of what has been accomplished and is eager to see how these outcomes will influence future endeavours in the field.

As we conclude, we would like to express our deepest gratitude to all partners, participants, the ECSEL Joint Undertaking, the participating countries and European Union for their continuous support throughout this journey. The success of the VALU3S "Final demo" showcases the power of collaboration and the pursuit of innovation.




## References

- [1] ERARGE et al., "Deliverable D5.6 - Evaluation report including the evaluation of the improved V&V processes as well as framework limitations," VALU3S Consortium, 2023.
- [2] CAMEA et al., "Deliverable D5.5 - Final Demonstrator Implementation Status Report," VALU3S Consortium, 2023.
- [3] COIMBRA et al., "VALU3S web-based repository," VALU3S Consortium, 11 2022. [Online]. Available: <https://repo.valu3s.eu/>. [Accessed 25 04 2023].




# Appendix A Demo Posters

## A.1 Use Case 1



Developed in Use Case 1 –  
Intelligent Traffic  
Surveillance



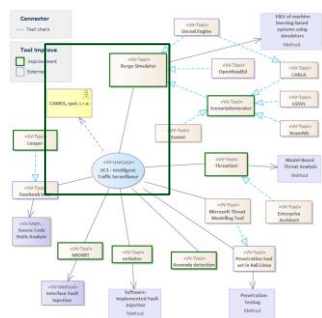
# V&V of License Plate Detection System

### Description of Demonstrator

Using machine learning (ML) components in critical applications introduces challenges for verification and validation (V&V) resulted by the opaque nature of ML. Inspired by **AMLAS** methodology (Assurance of Machine Learning in Autonomous Systems), the method "**V&V of machine learning-based systems using simulators (VMS)**" has been designed to work within intelligent transport systems (ITS) surveillance domain. This demonstration showcases the capability of a photo realistic simulator (here Berge Simulator) to model traffic scenarios for the purpose of validation and verification (V&V) of the **CAMEA Unicam** ML-based license plate recognition system. By comparing the sensor outputs obtained from the simulator with those obtained from real images captured at the scene, we can confirm that the simulator is a suitable tool for testing such systems. This has also been verified feeding simulated inputs to core processing components used in real traffic monitoring systems and comparing detection results with those obtained based on the real data input.



### Connection of the tool(s)



System requirements are allocated into ML-component requirements, which are then further broken down into V&V data requirements and ML requirements. The V&V data requirements are supported by the toolchain comprising of:

- An Unreal-engine based **Berge Simulator** that can reconstruct realistic sensor responses of V&V traffic scenarios in a traffic settings with scenario parameters set by ScenarioGenerator
- A **ScenarioGenerator** tool supporting various testing approaches, maps multidimensional Euclidean scenario vector spaces to the traffic scenarios in Berge Simulator.

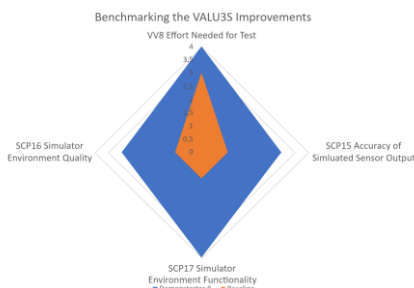
The toolchain generates synthetic labelled datasets that can be used to **validate the ML-based LP detector/recognition system**. Scenarios are generated with varying settings of illuminations, weather, sensor specification, mounting positions and different mobility patterns (vehicle trajectories) of the traffic spots of interest.

**Workflow in  
VALU3S  
repository**



### Evaluation

The main advantage of the V&V approach using traffic simulator-based vehicle detection is rapid verification and validation of traffic systems based on smart sensors (cameras or radars in this case).



### Expected Impacts

- Reduction of development costs, improved reliability, and faster time-to-market thanks to sensor inputs generated on demand
- Easier testing and validation of traffic monitoring and quality inspection systems thanks to scenario generator included in the tool
- Simplified modification and customization of traffic monitoring systems thanks to flexibility simulation tool that can be used for verification of traffic monitoring systems

### Related/ Impacted Standards

- ISO 26262, IEC 61508
- ISO 21448, UL4600, ISO PAS 8800, ISO DIS 34504
- ASAM OpenDRIVE®, OpenSCENARIO®
- AMLAS

### Involved VALU3S Partners

Leader: **CAMEA**

Participating Partners:



VALU3S HAS RECEIVED FUNDING FROM THE ECSEL JOINT UNDERTAKING UNDER GRANT AGREEMENT NO 876852. THE JOINT UNDERTAKING RECEIVES SUPPORT FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME AND AUSTRIA, CZECH REPUBLIC, GERMANY, IRELAND, ITALY, PORTUGAL, SPAIN, SWEDEN, TURKEY.

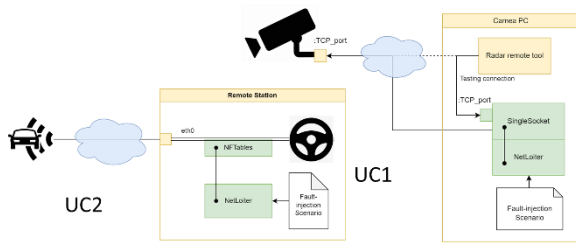




# Testing network communication using NetLoiter

## Description of Demonstrator

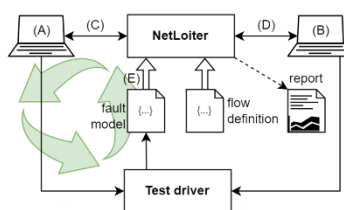
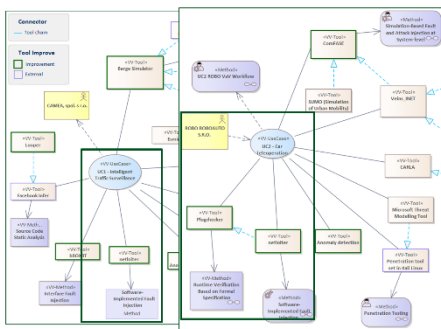
The demonstration *NetLoiter* is a tool providing the means for a systematic way of injecting faults into network traffic. The tool is used for experiments in test cases related to checking if a system-under-test performs correctly under different network conditions. Faults (i.e., unexpected conditions of network traffic) include network latency, lossy channel, packet reordering, jitter, and/or their combinations. The demonstration incorporates (i) CAMEA's smart radar sensor with *NetLoiter* configured to semi-automatically test different packet latencies and packet drop ratios in radar-specific net flows, (ii) as well as Roboauto's teleoperation system for automatic validation of requirements on network link reliability.



## Connection of the tool(s)

The tool can be applied to a network interface (virtual or a real one), letting it intercept communication, e.g., between a client and a server, an IoT device with its surroundings, and in a publish-subscribe broadcasting.

A test driver can control the tool using *NetLoiter*'s RestAPI (for managing fault models). Test feedback can be managed by *Plugchecker* verifying the correct system behaviour in run-time.

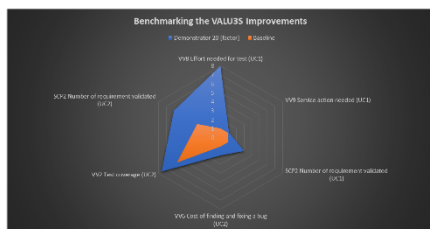


### Supported deployment:

- 1) HiL – Netloiter as a two-ethernet device (man-in-the-middle).
- 2) Hidden SW – uses virtual network, Linux kernel TC/NFT.
- 3) Visible SW – TCP/UDP proxy.

## Evaluation

The main advantage of the V&V approach to testing the network connectivity is (a) making it available to influence the behaviour of the network during testing and (b) the possibility of automating the V&V task.



- UC1: 1 out of 3 requirements related to the scenario:  
**Node connection to the cloud.** Effort for service actions reduced from 90 PH to 82 PH.
- UC2: 3 out of 7 requirements related to the scenario:  
**Transmission line under different performance conditions,** cost of fixing a bug from 5.5 to 3 hours, code coverage improved from 56% to 76%.

## Expected Impacts

- Reduction of development costs, improved reliability, and faster time-to-market.
- Easier testing and validation of traffic monitoring and quality inspection systems.
- Simplified modification and customisation of traffic monitoring systems.
- Automation during continuous integration/development.

## Related Standards

- ISO 26262 – Road vehicles – Functional safety
- ISO 29119-4 – Software testing – Test techniques

## Involved VALU3S Partners



Participating Partners:



VALU3S HAS RECEIVED FUNDING FROM THE ECSEL JOINT UNDERTAKING UNDER GRANT AGREEMENT NO 876852. THE JOINT UNDERTAKING RECEIVES SUPPORT FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME AND AUSTRIA, CZECH REPUBLIC, GERMANY, IRELAND, ITALY, PORTUGAL, SPAIN, SWEDEN, TURKEY.



## A.2 Use Case 2



# Use Case 2 Car Teleoperation



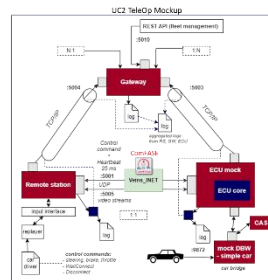
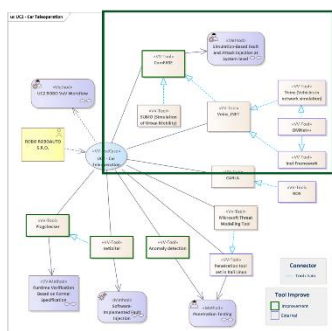
## V&V of Car Teleoperation under Faults and Attacks in Wireless Communication

### Description of Demonstrator

This demonstrator tackle challenges in performing fault and attack injection in wireless communication with a realistic mock-up of the system-under-test. Simulation of wireless network communication is used to ensure repeatability and control of the V&V process, while integrating with a mock-up of an actual software module to verify and validate systems under realistic operating conditions.



### Connection of the tool(s)



**Workflow in VALU3S repository**

- ComFASE tool implemented in Veins\_INET
- Veins\_INET simulates communication network between mock-up components (i.e., Remote station and ECU mock)
- Faults and attacks are injected into the teleoperated vehicle's communication network.

### Evaluation

The teleoperation system evaluation is carried out by injecting delay attacks and Denial-of-Service (DoS) attacks.

Tested the following basic requirements:

- When the front camera stream is disabled the vehicle safe stop should activate.
- When the control commands are disabled the vehicle safe stop should activate.
- When the delay is more than 0.15s the safestop should activate but the channel between the car and the RS (remote station) is not disconnected.
- When the delay is more than 1.5s the channel should be disconnected and the vehicle should stop (no speed).
- Introduced the varying delay and analyse the outcome.



### Expected Impacts

- Tested and verified the fallback mechanisms that are implemented in UC2 teleoperation system.
- Saved the test prep and execution time (i.e., testing in simulation Vs real-world testing).
- The time, cost and effort of performing fault and attack injection may be improved as well as the number of test cases by testing in simulation-based environment.
- Give a unique opportunity to the system designers to validate the functionality of their teleoperation application by injecting communication-based fault and attacks.
- Help the testers to choose the tests that should be carried out in real world environment.

### Related/Impacted Standards

No standardisation work within this demonstrator

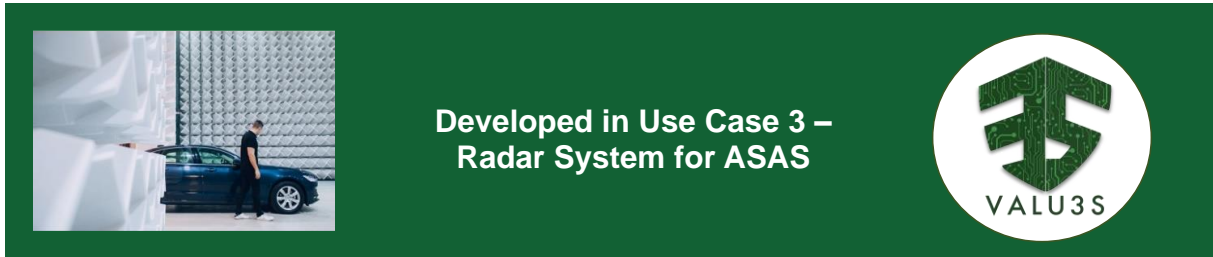
### Involved VALU3S Partners

Leader: **RI SE vti** Participating Partners: **roboauto**

VALU3S HAS RECEIVED FUNDING FROM THE ECSEL JOINT UNDERTAKING UNDER GRANT AGREEMENT NO 876852. THE JOINT UNDERTAKING RECEIVES SUPPORT FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME AND AUSTRIA, CZECH REPUBLIC, GERMANY, IRELAND, ITALY, PORTUGAL, SPAIN, SWEDEN, TURKEY.



### A.3 Use Case 3



Developed in Use Case 3 – Radar System for ASAS



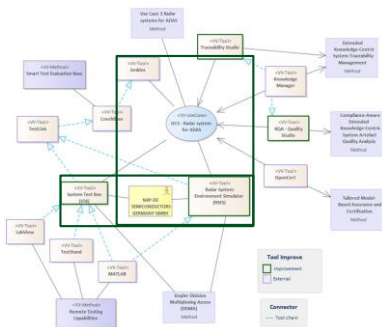
# Remote controlled radar target simulation and validation

## Description of Demonstrator

The RSES is utilised to simulate various real-world driving scenarios. However, due to the high cost and immobility of the equipment, the aim is to demonstrate the newly developed remote validation process that can be performed from the lab in Munich while being based in Porto. The goal is to allow global competence centres to use the hardware validation equipment in the future, making the validation process more resilient to external factors, such as a pandemic situation. Additionally, this approach reduces the overall cost and time required for validation, which accounts for approximately 80% of the total radar development cycle cost. The planned scenarios simulate different moving targets, validating a radar chip in a system environment with varying speeds, angles, ranges, and temperatures.



## Connection of the tool(s)

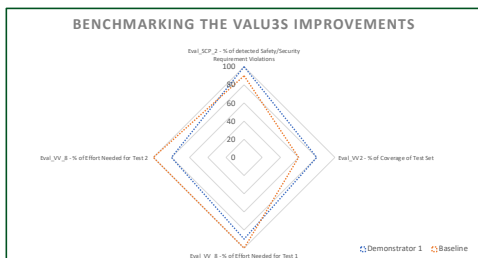


- Interaction between the developed tools RSES (a target simulator for radar targets in real world driving scenarios) and STB (System Test Box), and the method DDMA (Doppler Division Multiplexing Access). The combination of these three parts is the center of gravity for the innovations in the NXP V&V process as they are enabling the system validation at the IC supplier stage.
- The RSES is embedded in a tool suite including continuous integration tools such as Jenkins, a smart test evaluation data base and other supporting tools to increase the automation and efficiency of the Radar V&V process.

**Workflow in VALU3S repository**

## Evaluation of improvement

- Eval\_SCP\_2 – Number of Safety/Security Requirement Violations: The detection of bugs which could cause safety violations is improved by the RSES and System Test Box as test coverage also covers traffic scenarios.
- Eval\_VV\_2 – Coverage of Test Set: Integrating RSES to validate radar systems in traffic scenarios. Multiple targets with multiple parameters can be measured in traffic scenarios at Tier2
- Eval\_VV\_8-1 – Reduction of test effort: Remote testing capabilities for optimization of radar chip parameters. Impactful with restrictions to collaborate in person (e.g. pandemic) → workers can be off site
- Eval\_VV\_8-2 – Reduction of test effort: Integrating RSES to validate radar systems in traffic scenarios. Traffic scenarios can be simulated by the RSES → effort can be reduced.



## Expected Impacts

- Simulation based V&V will decreasing time and cost needed for radar development cycles whereas the complexity and quality standards are rising constantly. This will boost the competitiveness of the developed products and help to enable new ADAS functions more rapidly.
- The integration of simulation-based evaluation scenarios lay the ground work for potential future research projects on topics such as cooperative shared V&V models (while protecting individual IP)
- Further, remote testing capabilities aid the need for ubiquitous work in a multi-national, multi-continental company. Moreover, remote testing saves V&V budget as test benches haven't to be bought for every site but can be used globally.

## Related/ Impacted Standards

No standardisation work within this demonstrator

## Involved VALU3S Partners

Leader: **NXP**

VALU3S HAS RECEIVED FUNDING FROM THE ECSEL JOINT UNDERTAKING UNDER GRANT AGREEMENT NO 876852. THE JOINT UNDERTAKING RECEIVES SUPPORT FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME AND AUSTRIA, CZECH REPUBLIC, GERMANY, IRELAND, ITALY, PORTUGAL, SPAIN, SWEDEN, TURKEY.





## A.4 Use Case 4



**Developed in Use Case 4 –  
Human-Robot-Interaction  
in Semi-Automatic  
Assembly Processes**

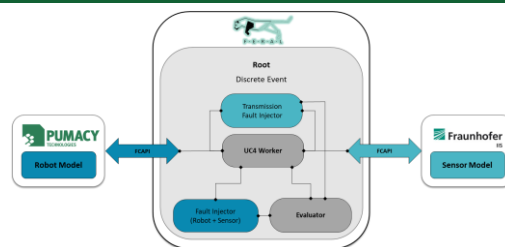


# Handling and Gripping of Products / Parts

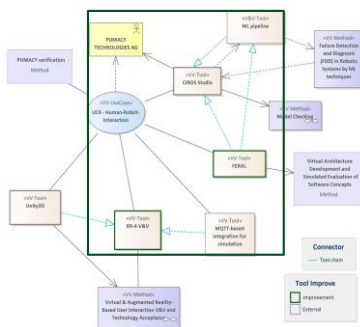
### Description of Demonstrator

"The demonstrator is based on a Human-Robot-Interaction (HRI) process taking place on the shop floor of a manufacturing-like environment. The process itself involves the execution of assembly tasks by human workers, focusing on the assembly of transformer units which consist of multiple parts. The demonstrator consist of the following two test cases that focus on the gripper of the robot without involvement of human worker:

"Remove product from simulation" (failure simulation) - (robot should stop immediately) and "Do not grip in simulation" (failure simulation)



### Connection of the tool(s)



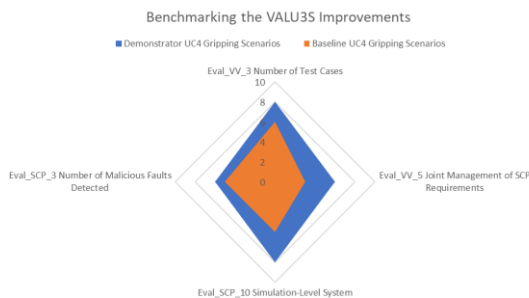
- By extending the simulation framework FERAL regarding its support for domain-specific communication protocols (OPC-UA), the connection to the simulator CIROS studio via a Python interface, and a fault injection component enables fault injection into simulation model within CIROS studio.
- XR-4-V&V system allows human workers to collaborate with industrial robots in a simulated environment through the use of a head-mounted display. XR-4-V&V is using the Unity3D platform and focuses on handling only human interaction. Meanwhile, the robot simulation model runs on the CIROS studio, and the communication between the two will be facilitated by FERAL, utilizing MQTT for message exchange.

**Workflow in  
VALU3S  
repository**



### Evaluation

By using dedicated simulation models and fault injection, several functional and non-functional requirements (esp. fault tolerance and robustness) can be checked. By extending the fault model, the detection rate of additional fault types can be increased.



### Expected Impacts

- Simplified approach to verify and validate the safety and security of HRI systems
- Reduced effort for system certification
- The reduction in the price of robotics system approval will allow more and more companies to opt for its use

### Related/ Impacted Standards

- ISO 10218-2:2011 (Robots and robotic devices — Safety requirements for industrial robots)
- ISO/TS 15066 (Technical Specification Robots and Robotics - Collaborative Robots)
- IEC 61508:2010 (Functional Safety)

### Involved VALU3S Partners

Leader: **Fraunhofer**

Participating Partners:



VALU3S HAS RECEIVED FUNDING FROM THE ECSEL JOINT UNDERTAKING UNDER GRANT AGREEMENT NO 876852. THE JOINT UNDERTAKING RECEIVES SUPPORT FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME AND AUSTRIA, CZECH REPUBLIC, GERMANY, IRELAND, ITALY, PORTUGAL, SPAIN, SWEDEN, TURKEY.





## A.5 Use Case 5



Developed in Use Case 5 – Aircraft Engine Controller



# Model based Design and Validation of the Hybrid Model

### Description of Demonstrator

The aim of the demonstrator is to obtain certified proof of stability of hybrid systems by use of symbolic techniques. The use case considered is a hybrid system with two modes, each one consisting of an affine dynamical system.

The evaluation focuses on two different aspects: the synthesis of a robust region (with fixed reference values), and robustness to reference values changes. We approach these two targets by use of the tool Sabbath, that is integrated into an ad-hoc script.

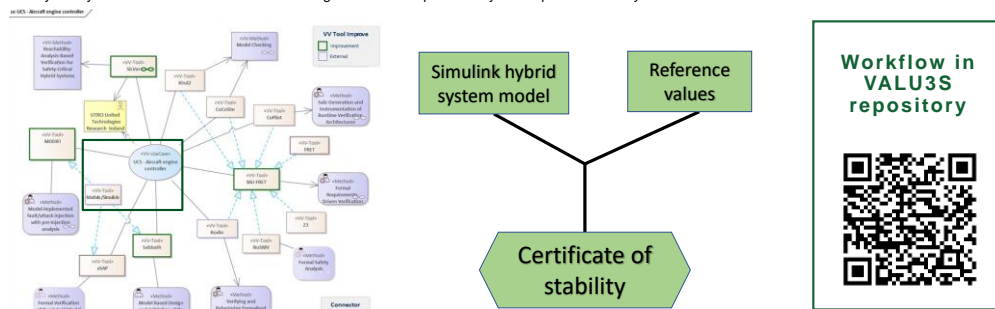
One essential tool in the symbolic proof is the numerical synthesis of quadratic Lyapunov functions and their validation by means of symbolic calculus and SMT-solvers.

```

$ cd /home/.../...
$ python3 verify_po.py --solver z3 --use-exponential --size 5
-> Read matrices
A size 5x5
B size 5x2
C size 4x5
-> Controller matrices
K1 size 3x4
K2 size 3x4
K3 size 3x4
INFO: main...Reference values: [1/2, 5.0, -1.0, 20.0]
INFO: main...Finding assumptions...
INFO: main...Searching a Lyapunov function candidate...
CRITICAL:root:Synthesizing Lyapunov with exponential
CRITICAL:root:found alpha = 4.19
CRITICAL:root:solving with cvopt
    
```

### Connections of the tool

The hybrid system is described in Simulink and is given to our script to find symbolic proof of stability.



### Evaluation

The tool gives a way to obtain regions of certified stability for a piecewise affine dynamical system. The candidate Lyapunov function used to achieve this task can be numerically synthesized in different ways. Once we have such a function, we can use various tools (symbolic techniques or SMT solvers) to certify its validity.

The results obtained by comparing these methods are presented in the table. The figure represents the number of validated instances over time by the symbolic methods.

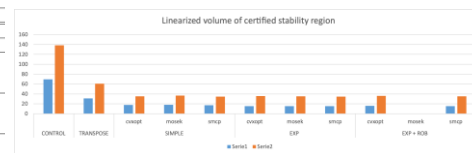
method	solver	size 15			mode 1			size 18			mode 1		
		time	vol	ε	time	vol	ε	time	vol	ε	time	vol	ε
eq-num		286	7e-10	7e-7	235	1e-4	2e-6	808	5e+38	4e-9	916	9e+44	1e-8
modal		161	7e-18	3e-6	148	7e-10	1e-5	680	2e+31	2e-10	679	3e+37	5e-10
LMI	cvxopt	302	8e+0	3e-5	307	1e+6	7e-5	642	2e+26	3e-8	569	3e+32	8e-8
LMI	mosoc	321	9e+0	3e-5	324	1e+6	6e-5	707	3e+26	3e-8	713	7e+32	8e-8
LMI	smcp	295	9e+0	3e-5	310	1e+6	7e-5	558	9e+25	2e-8	547	2e+32	7e-8
LMIα	cvxopt	309	1e+1	2e-5	199	1e+6	5e-5	769	1e+25	2e-8	594	4e+32	6e-8
LMIα	mosoc	189	8e+0	2e-5	167	1e+6	5e-5	692	1e+25	2e-8	692	3e+32	6e-8
LMIα	smcp	226	1e+1	2e-5	198	1e+6	5e-5	747	7e+24	1e-8	799	2e+32	6e-8
LMIα*	cvxopt	276	1e+0	2e-5	281	1e+5	5e-5	803	2e+25	2e-8	731	5e+32	7e-8
LMIα*	mosoc	255	6e+0	3e-5	280	8e+5	7e-5	-	-	-	-	-	-
LMIα*	smcp	257	5e+0	2e-5	198	7e+5	6e-5	555	1e+25	2e-8	760	3e+32	7e-8

### Expected Impacts

- Symbolic verification of stability will improve the safety of the systems.
- Finding a certified proof of stability can lower the amount of tests needed.

### Related/ Impacted Standards

No standardisation work within this demonstrator



### Involved VALU3S Partners

Leader:



Participating Partners:



VALU3S HAS RECEIVED FUNDING FROM THE ECSEL JOINT UNDERTAKING UNDER GRANT AGREEMENT NO 876852. THE JOINT UNDERTAKING RECEIVES SUPPORT FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME AND AUSTRIA, CZECH REPUBLIC, GERMANY, IRELAND, ITALY, PORTUGAL, SPAIN, SWEDEN, TURKEY.





Developed in Use Case 5 – Aircraft Engine Controller

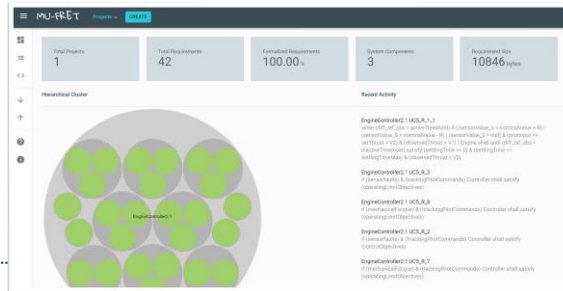


# Mu-FRET Demonstration

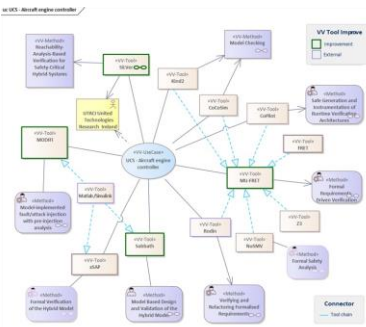
## Verifying and Refactoring Formalised Requirements

### Description of Demonstrator

Requirements are often expressed in natural language, and often at a level of detail that is not suitable for direct formalisation. A semi-formal language may be used as an intermediate between natural- and formal-languages, which avoids slowing down the requirements elicitation process, but still provides enough formalisation to both reduce ambiguities and make the requirements easier to (fully) formalise later on. This addresses one common criticism of formal methods; that they are too abstract and too far removed from realistic models used for designs and simulations



### Connection of the tool(s)



- FRET allows for requirements to be stated in a structured natural language called FRETISH.
- MU-FRET expands on this by implementing refactoring techniques, improving the requirements elicitation process.
- From these FRETISH requirements, we can generate contracts in CoCoSim, which can be attached to a Simulink diagram to be used for model checking.
- The requirements and diagram are also used as the basis for an independent system model in Event-B.

Mu-FRET on the VALU3S repository      Workflow on the VALU3S repository



### Evaluation

Our FRETISH requirements set is derived from the 14 English-language requirements and 20 abstract test cases provided by Collins Aerospace. We mapped the natural-language requirements, one-to-one, to 14 FRETISH parent requirements. The child requirements add detail from the test cases and elicitation discussions; we produced a set of 28 child requirements. We identified seven definitions that were repeated in multiple child requirements, which we call fragments. We make use of the Extract Requirement refactoring (GUI element included, right) to separate these fragments into their own requirements, which reduces repetition and improves readability. It also allows us to remove redundant requirements; after refactoring, there were twelve identical child requirements that could be removed. The details on the fragments are included in the table below.

ID	Fragment Name	N of (Re)Definitions	
		Before Refactoring	After Refactoring
F1	Sensor Faults	9	1
F2	Tracking Pilot Commands	13	1
F3	Control Objectives	18	1
F4	Regulation Of Nominal Operation	14	1
F5	Operating Limit Objectives	6	1
F6	Mechanical Fatigue	9	1
F7	Low Probability Hazardous Events	9	1
F8	Active	28	1
F9	Not Active	28	1
<b>Total (Re)Definitions</b>		<b>132</b>	<b>9</b>



### Expected Impacts

- Formalised requirements are easier to input/translate into languages used by formal methods.
- The act of formalising the requirements highlights ambiguities that may cause problems later in the development process.

### Related/ Impacted Standards

No standardisation work within this demonstrator

### Involved VALU3S Partners



Participating Partners:



VALU3S HAS RECEIVED FUNDING FROM THE ECSEL JOINT UNDERTAKING UNDER GRANT AGREEMENT NO 876852. THE JOINT UNDERTAKING RECEIVES SUPPORT FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME AND AUSTRIA, CZECH REPUBLIC, GERMANY, IRELAND, ITALY, PORTUGAL, SPAIN, SWEDEN, TURKEY.





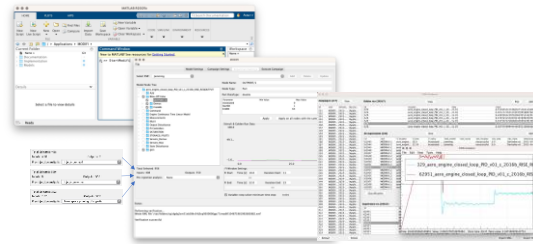
## Developed in Use Case 5 – Aircraft Engine Controller



# Model-Implemented Fault/Attack Injection with Pre-Injection Analysis

### Description of Demonstrator

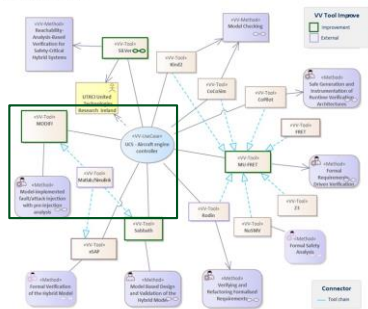
- Improvements obtained with pre-injection analysis for model-implemented fault- and attack injection are demonstrated.
- The pre-injection analysis is used for reducing the error space to improve the efficiency of the fault- and attack injections.
- The pre-injection analysis is applied on a Simulink model of the UC5 aero engine controller using the MODIFI tool.
- The improvements in terms of time and effort needed to conduct the injections are comparable to the reduction of the error space achieved by the pre-injection analysis.



### Connection of the tool(s)

The MODIFI (Model-Implemented Fault- and attack Injection) tool supports model-implemented fault- and attack injection methods within MATLAB/Simulink.

uc5 - uc5 aero engine controller



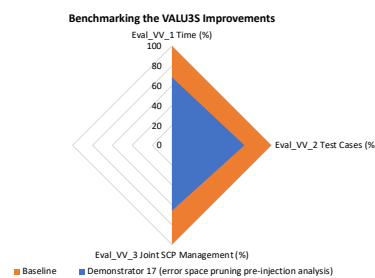
- MODIFI is started from the MATLAB command window which brings up the MODIFI GUI where the fault- and attack injection campaigns, including pre-injection analyses such as *inject-on-read*, *inject-on-write* and *error space pruning of signals*, may be configured and executed.
- MODIFI allows different fault- and attack injection mechanisms implemented as Simulink blocks to be injected into the target system model and control how the model is simulated by Simulink.
- MODIFI monitors selected signals of the target system model when the model is simulated by Simulink and collects the monitored data in an internal database for subsequent analysis.

Workflow in VALU3S repository



### Evaluation

The diagram below shows the improvements in terms of time of test execution, number of test cases and joint management of safety, cybersecurity and privacy using error space pruning of signals pre-injection analysis when injecting noise faults into the UC5 aero engine controller with the MODIFI tool.



### Expected Impacts

- The number of test cases is reduced by 27% for error space pruning of signals pre-injection analysis.
- The reduction of the test execution time is comparable to the reduction of the number of test cases due to negligible pre-injection analysis time.
- Joint management of safety, cybersecurity and privacy is also improved, since both safety and cybersecurity requirements may be verified jointly when injecting fault- or attack models which are considered equivalent.
- These improvements are expected to reduce the time and cost of performing injection-based V&V.

### Related/Impacted Standards

- DO-178C: Software Considerations in Airborne Systems and Equipment Certification
- IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems
- ISO 26262: Road vehicles — Functional safety
- ISO/SAE 21434: Road vehicles — Cybersecurity engineering
- ISO 13849: Safety of machinery – Safety-related parts of control systems

### Involved VALU3S Partners



Participating Partners: Collins Aerospace

VALU3S HAS RECEIVED FUNDING FROM THE ECSEL JOINT UNDERTAKING UNDER GRANT AGREEMENT NO 876852. THE JOINT UNDERTAKING RECEIVES SUPPORT FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME AND AUSTRIA, CZECH REPUBLIC, GERMANY, IRELAND, ITALY, PORTUGAL, SPAIN, SWEDEN, TURKEY.



ECSEL Joint Undertaking





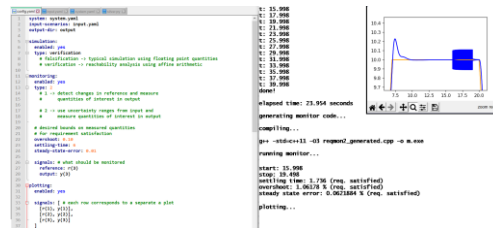
## Developed in Use Case 5 – Aircraft Engine Controller



# SiLVer – SimuLation-based Verification

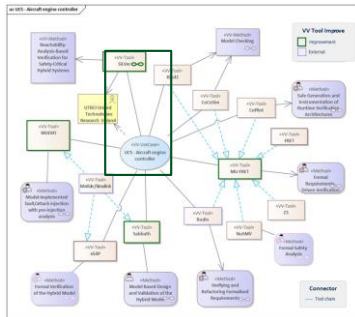
### Description of Demonstrator

- The aim of the demonstrator is showcasing the SiLVer tool features in an end-to-end way: Starting with requirement and system model templates, as well as configuration parameters, generating and running the corresponding C++ code, as well as plotting the obtained results.
- The developed workflow aims to be a near-drop-in replacement for Monte Carlo simulation, providing better coverage (through interval analysis) and at the same time reduced test execution time. Using C++ code as the analysis target enables evaluation throughout the system design process. Parametrizable templates are provided to ease translation of requirements and system model.



### Connection of the tool(s)

The SiLVer tool supports interval-based reachability analysis of C++ code, in order to determine system conformance with respect to requirements.

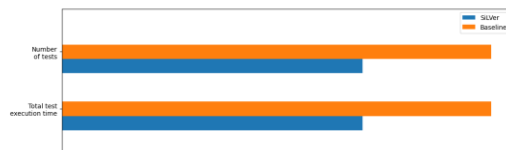


- The SiLVer tool is implemented as a set of Python scripts that generate and run C++ code. Configuration information and tool input are provided using a set of YAML files.
- Facilitating translation of Simulink models for analysis is done through providing C++ template files, parametrizable through corresponding YAML files.
- Similarly, parametrizable templates for control requirements (e.g. overshoot, settling time, steady state error, etc.) are provided in order to facilitate requirement translation.

**Workflow in VALU3S repository**

### Evaluation

- Core improvements the SiLVer tool provides through interval analysis against the Monte Carlo simulation baseline are in number of test cases as well as total test execution time required for obtaining similar coverage. The measured reduction in both cases is typically more than 30% and the observed gain typically increases as the number of dimensions in the system under analysis increases.



- Other, more qualitative, improvements include easier (more automated) translation of requirements into a form able to be used for analysis, as well as reduced overall effort for certification, as a direct result of all above mentioned improvements.

### Expected Impacts

- Improved test execution time and reduced number of test cases.
- Improved V&V automation & applicability
- Reduced overall effort for certification

### Related Standards

- DO-178C: Software Considerations in Airborne Systems and Equipment Certification
- DO-333 – Formal Methods (Supplement to DO-178C)

### Involved VALU3S Partners

Leader: Collins Aerospace

VALU3S HAS RECEIVED FUNDING FROM THE ECSEL JOINT UNDERTAKING UNDER GRANT AGREEMENT NO 876852. THE JOINT UNDERTAKING RECEIVES SUPPORT FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME AND AUSTRIA, CZECH REPUBLIC, GERMANY, IRELAND, ITALY, PORTUGAL, SPAIN, SWEDEN, TURKEY.

ECSEL Joint Undertaking  
Electronic Components and Systems for European Leadership



## A.6 Use Case 6



**Developed in Use Case 6–  
Agricultural Robot**

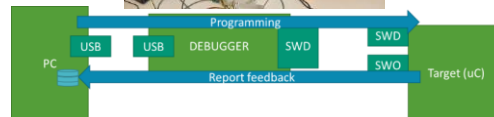


# Arm Unity

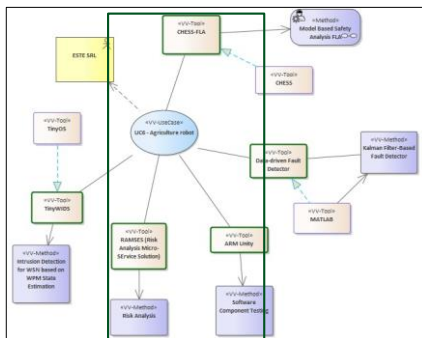
### Description of Demonstrator

Demonstration of software component testing using open-source SW framework adapted during the VALU3S project to be executed directly in target device instead of be executed on PC.

With this approach the SW test and HW/SW integration test, requested by ISO 26262 and ISO 25119, are executed in the same test step, improving the Effort needed for test valu3s' VV evaluation criteria.



### Connection of the tool(s)



Arm Unity is an enhancement of the open source unit test framework Unity. Arm Unity is tailored for embedded system resources and performs Unit Test on target device creating the test report of tests execution to PC.

Arm Unity improves the test relevance using same environment (compiler + uC) of the production executing SW test and HW/SW integration test in the same test step.

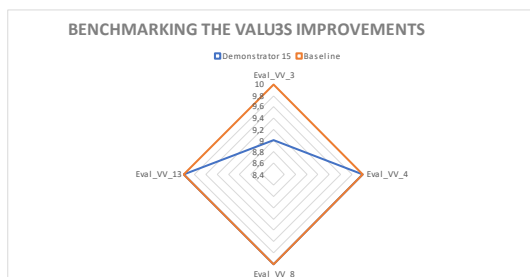
The Arm Unity tool is executed to verify the code relevant for safety and cybersecurity. RAMSES and CHES-FLA outputs are used to define the safety and cybersecurity relevant code.

Use Case in  
VALU3S  
repository



### Evaluation

The gain comes by not creating specific HW/SW integration tests, avoid stub function for HW part during SW component testing executed on PC, avoid the creation of dedicated linker file to execute unit test on PC.



### Expected Impacts

- Effort needed for test improved for safety or cybersecurity relevant code

### Related/ Impacted Standards

- ISO 25119: SW test and HW/SW integration test
- ISO 26262: SW test and HW/SW integration test

### Involved VALU3S Partners

Leader:



Participating Partners:



VALU 3S HAS RECEIVED FUNDING FROM THE ECSEL JOINT UNDERTAKING UNDER GRANT AGREEMENT NO 876852. THE JOINT UNDERTAKING RECEIVES SUPPORT FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME AND AUSTRIA, CZECH REPUBLIC, GERMANY, IRELAND, ITALY, PORTUGAL, SPAIN, SWEDEN, TURKEY.





## Developed in Use Case 6 – Agricultural Robot



# Risk analysis with RAMSES tool

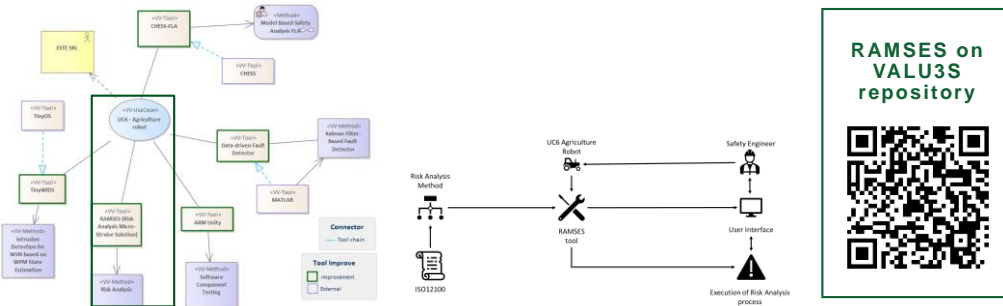
### Description of Demonstrator

RAMSES is demonstrated in UC6 to support Risk Management of the Agriculture Robot design following ISO12100 prescriptions. The user (i.e. the safety engineer) can create and assess hazardous scenarios related to the usage of the machine. Then, risk of each scenario can be mitigated when necessary to be compliant with standard by introducing new safety measures that can reduce the risk score. The objective of this demonstrator, indeed, is to show that risk analysis process can be significantly improved by ensuring standard compliance and higher safety standards while reducing time and cost needed to undertake the whole process.



### Connection of the tool(s)

RAMSES tool implements the Risk Analysis method following ISO12100 prescriptions. The use-case should be modelled on the tool through the UI; in the same way, the user can undertake the whole risk analysis process by following RAMSES wizards.



### Evaluation

- Use Case 6:
  - 4 evaluation scenarios addressed
  - 2 SCP evaluation criteria addressed
  - 1 V&V evaluation criteria addressed
  - 20+ risk scenarios modelled and evaluated for the use-case

### Expected Impacts

- 33% reduction of the effort (i.e. Man Months) needed to undertake risk analysis during design of the automated system
- 68% increase of safety scenarios considered within the risk analysis process

### Related/ Impacted Standards

RAMSES implements the risk analysis methodology defined in ISO 12100 standard, that addresses safe design of machine. The tool can be easily customised on similar standards

### Involved VALU3S Partners

Leader: MASTERING EXCELLENCE Participating Partners:

VALU3S HAS RECEIVED FUNDING FROM THE ECSEL JOINT UNDERTAKING UNDER GRANT AGREEMENT NO 876852. THE JOINT UNDERTAKING RECEIVES SUPPORT FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME AND AUSTRIA, CZECH REPUBLIC, GERMANY, IRELAND, ITALY, PORTUGAL, SPAIN, SWEDEN, TURKEY.







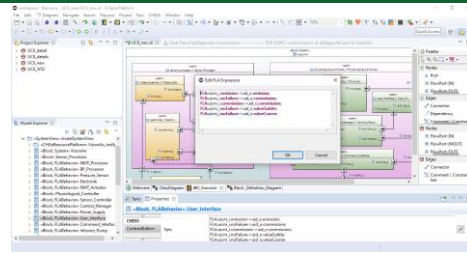
Developed in Use Case 6 –  
Agricultural Robot &  
Use Case 8 –  
Infusion Controller of NMT



# MSA-FLA with CHESS-FLA

## Description of Demonstrator

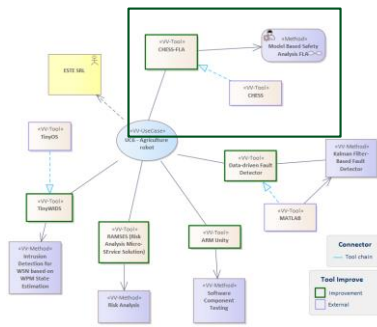
Demonstration of the application of the CHESS-FLA tool on the UC6 and UC8 systems. Starting from the designed functional model of the systems, we will show how to apply the Failure Logical Analysis; that is how to describe the faulty behavior of the functional subsystems through the FLA rules. Once described the faulty behavior of the subcomponents, we will show how to qualitatively and quantitatively compute the faulty behavior of the entire system with the automatic generation of the FMEA (Failure Mode and Effect Analysis) table and the FTs (Fault Trees) and computing the probability of occurrence of the top events.



## Connection of the tool(s)

- CHESS-FLA is a CHESS plug-in improved in VALU3S that supports Model-Based Safety Analysis with Failure Logical Analysis.
- The MSA-FLA method has been applied to both UC6 and UC8 in the concept phase to analyse the potential hazard situations and later to test the effect of potential hazards

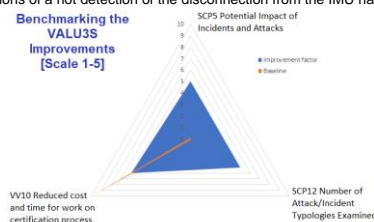
SYSTEM PATH	FUNCTION	FAILURE MODES	LOCAL EFFECTS	END EFFECTS
VisioAir.physiological_controller_1.Cable_1	Commission	Commission failure	Commission failure at start_port	VisioAir.diagnostic commission
VisioAir.physiological_controller_1.Cable_1	Commission	Commission failure	Commission failure at start_port	VisioAir.diagnostic commission
VisioAir.physiological_controller_1.Cable_1	Commission	Commission failure	Commission failure at start_port	VisioAir.diagnostic commission
VisioAir.physiological_controller_1.Cable_1	Commission	Commission failure	Commission failure at start_port	VisioAir.diagnostic commission



**Workflow in VALU3S repository**

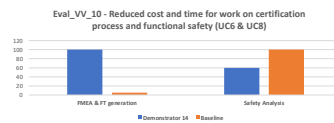
## Evaluation

- Use Case 8:**
  - 9 potential hazard situations deriving from the erroneous behavior of the Controller and 72 sequences or combination of events that may cause a hazard situation have been identified, 6 different characteristics that could affect the safety of the Controller have been analyzed.
- Use Case 6:**
  - 10 different consequences of a not detection of the disconnection from the remote control and 4 different situations of a not detection of the disconnection from the IMU have been analyzed.



## Expected Impacts

- Reduction of the error proneness due to the manual computation of the safety analysis artefacts
- Easy analysis of the effect of an injected fault on the system outputs



## Related/ Impacted Standards

The improved method (MSA-FLA) with its supporting tool (CHESS-FLA) could help system developers to reach compliance to safety standards in all safety-critical domains

- IEC 61508
- EN 50129
- ISO 26262
- ISO 14971

## Involved VALU3S Partners



Participating Partners:




VALU3S HAS RECEIVED FUNDING FROM THE ECSEL JOINT UNDERTAKING UNDER GRANT AGREEMENT NO 876852. THE JOINT UNDERTAKING RECEIVES SUPPORT FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME AND AUSTRIA, CZECH REPUBLIC, GERMANY, IRELAND, ITALY, PORTUGAL, SPAIN, SWEDEN, TURKEY.




ECSEL Joint Undertaking



## A.7 Use Case 7



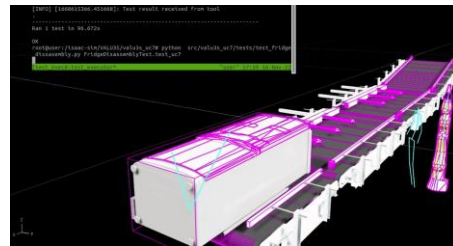
Developed in Use Case 7 –  
Human-Robot Collaboration in a  
Disassembly Process with Workers  
with Disabilities



# Coordination of Test Generation and Validation in Simulation-based Human-Robot Collaborative Environments

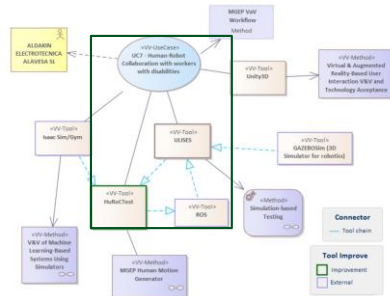
### Description of Demonstrator

Coordination of test generation and validation in simulation-based human-robot interaction environments (HuRoCTest) coordinates simulation-based testing activity in human-robot interaction environments. The HuRoCTest tool provides a real-time, automated verdict of test execution of simulation environments through constrained based-oracles using simulation-based testing for human-robot interaction. To coordinate the testing with the constrained-based oracle, HuRoCTest leverages a ROS package to seamlessly align the execution of the test, the simulation environment, and the oracle.



### Connection of the tool(s)

HuRoCTest employs three supporting tools to validate the correctness of a reinforcement learning control policy under test, as well as other safety and functionality requirements of any industrial facility in a human-robot interaction context.

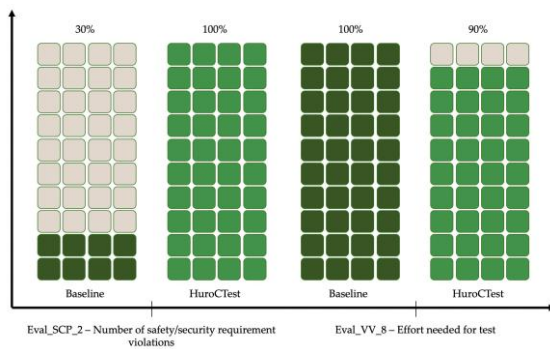


**Workflow in  
VALU3S  
repository**



- **NVIDIA Isaac Sim.** Simulation environment for the validation of the reinforcement learning control policy. The policy extracts a peg that mimics the magnetic gasket of a refrigerator door to the opposite site of the human to avoid a potential collision.
- **ROS.** The control policy is executed in a ROS environment. The test suite is implemented in Python and also runs in ROS.
- **ULISES.** Procedural-task evaluation approach for testing simulation-based human-robot interactions. This tool uses constraint-based modelling to implement the evaluation. These approaches usually receive as input models required to generate a diagnosis and data streams from the simulated system. The data from the ROS system is received through a ROS-MQTT bridge. After performing the evaluation, the result of the activity diagnosis is provided as output.

### Evaluation



### Expected Impacts

- Real-time test artefacts and diagnosis generation and coordination.
- No human-in-the-loop required.
- Coverage of a larger number of test cases.


### Related/ Impacted Standards

- **ISO 10218-1.** Robots and robotic devices. Safety requirements for industrial robots – Part 1: Robots.
- **ISO 10218-2.** Robots and robotic devices. Safety requirements for industrial robots – Part 2: Robot systems and integration.
- **ISO/TS 15066.** Robots and robot devices – Collaborative robots.

HuRoCTest allows real-time assessment in simulation of the safety requirements of the four types of collaborative operation referred to in the three standards.

### Involved VALU3S Partners

Leader:  **Mondragon Unibertsitatea**  
Professional Learning Space

Participating Partners:  **ALDAKIN**

VALU3S HAS RECEIVED FUNDING FROM THE ECSEL JOINT UNDERTAKING UNDER GRANT AGREEMENT NO 876852. THE JOINT UNDERTAKING RECEIVES SUPPORT FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME AND AUSTRIA, CZECH REPUBLIC, GERMANY, IRELAND, ITALY, PORTUGAL, SPAIN, SWEDEN, TURKEY.

 **ECSEL Joint Undertaking**  
Electronic Components and Systems for European Leadership



## A.8 Use Case 8



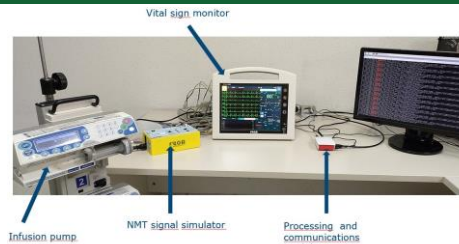
Developed in Use Case 8 –  
Infusion Controller of NMT



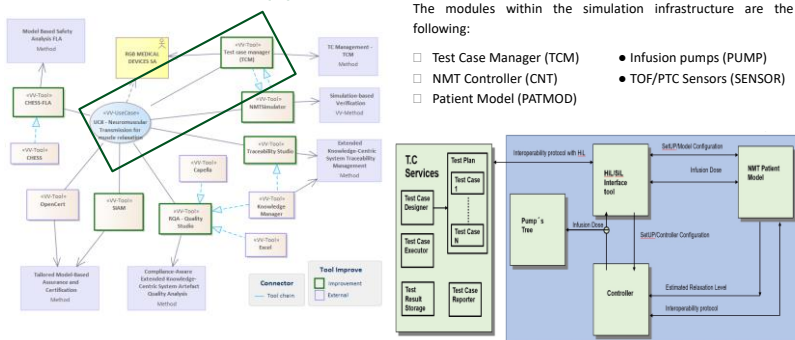
# NMT Simulator

### Description of Demonstrator

This demonstrator is a Testbench platform that can support in defining the algorithm that provides the best performance in NMT (NeuroMuscular Transmission) control. It makes use of a Patient's Model that provides the response of the patient (in NMT units) to a given dose infusion during the control period. Once this algorithm is defined, then it can be embedded in a real life Multiparameter monitor called Vision Air. NMTSimulator represents a comprehensive experimental platform for development of medical devices in the field of automated infusion of particular drugs. Since there are enormous obstacles in obtaining medical data for such development, simulating the problem is the only chance to move forward. NMTSimulator implements a control loop integrating an infusion pump, measurement sensor, target patient and the control device itself.



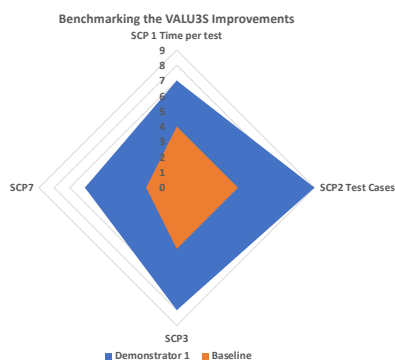
### Connection of the tool(s)



**Workflow in VALU3S repository**



### Evaluation



### Expected Impacts

1. Eval\_SCP\_1 – Error Coverage – the metric is used for evaluating the percentage of time that a “good” control is achieved.
2. Eval\_SCP\_2 – Number of Safety/Security Requirement Violations - the metric is planned for evaluating the level of deviation when the control is not within pre-established targets.
3. Eval\_SCP\_3 – Reduction of development costs, improved reliability, and faster time-to-market
4. Eval\_SCP\_7 – Number of Prevented Accidents will be used to select the proper test cases to cope with specific operating conditions that can be cause of accidents.

### Related/ Impacted Standards

Verified the applicability of the standard for this UC:

- EN ISO 14971: Risk Management
- EN 60601-1: Medical Electrical Devices applies to the basic safety and essential performance of any type of medical electrical device
- EN 62304: Medical Device Software It applies to the development and maintenance of medical device software
- EN 62366-1: Usability Engineering specifies a process for a manufacturer to analyse, specify, develop and evaluate the usability of a medical device as it relates to safety
- MDCG 2019-16: Guidance on Cybersecurity There are not any harmonized standard on cybersecurity, but it is a requirement of 2017/45 regulation

### Involved VALU3S Partners



VALU3S HAS RECEIVED FUNDING FROM THE ECSEL JOINT UNDERTAKING UNDER GRANT AGREEMENT NO 876852. THE JOINT UNDERTAKING RECEIVES SUPPORT FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME AND AUSTRIA, CZECH REPUBLIC, GERMANY, IRELAND, ITALY, PORTUGAL, SPAIN, SWEDEN, TURKEY.





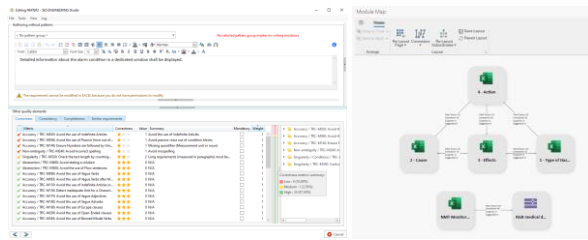
Developed in Use Case 8 –  
Infusion Controller of NMT



# Early V&V in Knowledge-Centric Systems Engineering

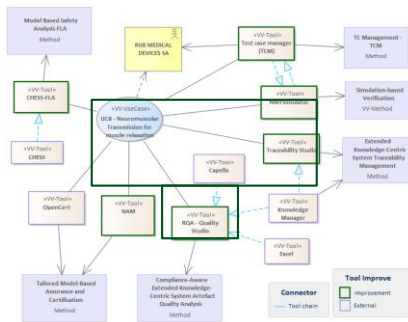
## Description of Demonstrator

- KCSE specialises model-based systems engineering with the idea that all systems engineering processes can benefit from knowledge bases about a system and its lifecycle
- Two KCSE methods have been improved in VALU3S for early V&V: (1) **Compliance-Aware Extended Knowledge-Centric System Artefact Quality Analysis** and (2) **Extended Knowledge-Centric Traceability Management**
- The methods and their supporting tools have been applied with UC8 data:
  - **Risks analysis**
  - **System models**
  - **Applicable standards**



## Connection of the tool(s)

The main tools of the demonstrator are **RQA - Quality Studio** and **Traceability Studio**. Capella, Excel, and Knowledge Manager are used as well.

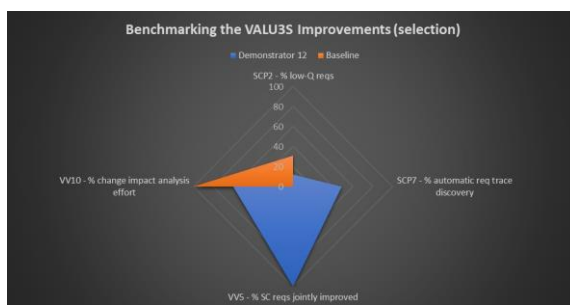


- Quality analysis of risk analysis info with RQA
- Model (Capella diagrams) quality analysis with RQA
- Improvement of risk analysis info with RQA
- Trace verification for risk info with Traceability Studio
- Trace discovery for risk info with Traceability Studio
- Change impact analysis for risk info with Traceability Studio
- Trace discovery for models with Traceability Studio



## Evaluation

Number of Safety/Security Requirement Violations (SCP2), Number of prevented accidents (SCP7), Joint management of SCP requirements (VV5), and Reduced cost and time for work on certification process and functional safety (VV10) have been used to evaluate the application of the methods and tools.



## Expected Impacts

- Wider system artefact quality analysis
- More precise traceability management
- Better system artefacts
- Lower effort in the addressed V&V tasks thanks for automated support
- Lower cost in issue resolution thanks to early issue detection

## Related/ Impacted Standards

- IEC 62304. Medical device software - Software life cycle processes
- IEC 14971. Medical devices - Application of risk management to medical devices

## Involved VALU3S Partners

Leader:



Participating Partners:



VALU3S HAS RECEIVED FUNDING FROM THE ECSEL JOINT UNDERTAKING UNDER GRANT AGREEMENT NO 876852. THE JOINT UNDERTAKING RECEIVES SUPPORT FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME AND AUSTRIA, CZECH REPUBLIC, GERMANY, IRELAND, ITALY, PORTUGAL, SPAIN, SWEDEN, TURKEY.



ECSEL Joint Undertaking

Electronic Components and Systems for European Leadership



## A.9 Use Case 9



Developed in Use Case 9 –  
Autonomous Train Operation



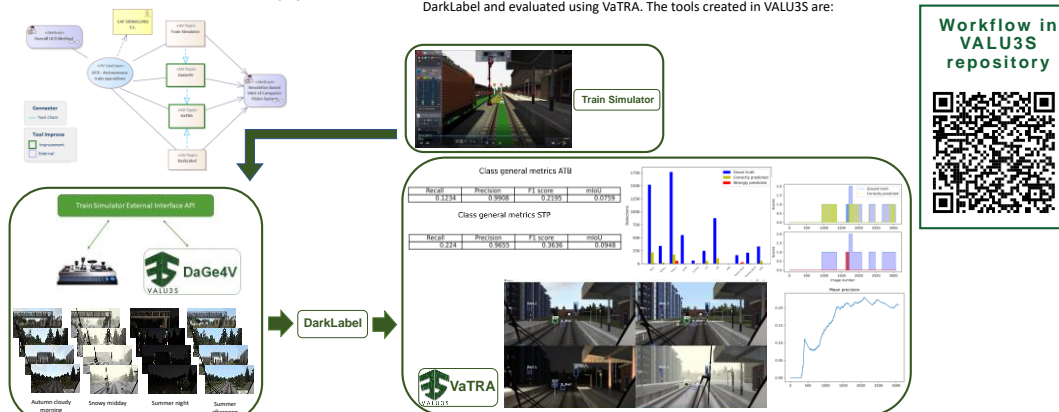
# Validation of Computer Vision system for railway using synthetic data

### Description of Demonstrator

CAF Signalling is currently working on a future GoA4 (driverless) Autonomous Train Operation (ATO) and is facing up different Verification and Validation (V&V) challenges for the CV&AI-enhanced autonomous train operations that are based on non-deterministic algorithms. It is not easy to collect a real database containing different realistic scenarios to validate computer vision-based AI techniques. There is a need to use simulation scenarios to ensure the reliability and fasten the system validation. This demonstration will show how the problem was crafted and which are the results obtained and the expected impacts.

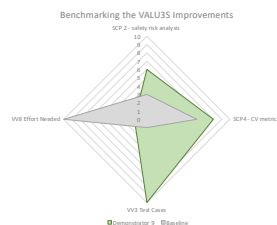


### Connection of the tool(s)



### Evaluation

The process of capturing railway frames is expensive in terms of time and resources and the diversity of the created scenarios is impossible to replicate in real life. Used evaluation scenarios are VALU3S\_WP1\_Railway\_4, 5 and 6. For evaluation, Eval\_SCP\_2 (helps in the risk analysis for safety and security), Eval\_SCP\_4 (measuring the model with Computer Vision metrics automatically enhances time and cost), Eval\_VV\_3 (increased by 10 the number generated tests), Eval\_VV\_8 (optimized by a factor of 25 time needed for creating a test scenario).




### Expected Impacts

- Reducing times and costs of diverse test scenario creation by improvement Eval\_VV\_8.
- Get immersed in new V&V methods for safety by Eval\_SCP\_2.
- Reduce the cost of validation of a CV&AI system by Eval\_SCP\_4.

### Related/ Impacted Standards

No standardisation work within this demonstrator

### Involved VALU3S Partners

Leader:  Participating Partners: 

VALU3S HAS RECEIVED FUNDING FROM THE ECSEL JOINT UNDERTAKING UNDER GRANT AGREEMENT NO 876852. THE JOINT UNDERTAKING RECEIVES SUPPORT FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME AND AUSTRIA, CZECH REPUBLIC, GERMANY, IRELAND, ITALY, PORTUGAL, SPAIN, SWEDEN, TURKEY.

 ECSEL Joint Undertaking  
Electronic Components and Systems for European Leadership



## A.10 Use Case 10

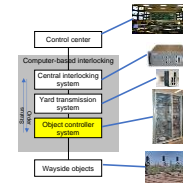


# Safety verification and validation for the signalling railway application

### UC 10 – Safety function out-of-context

For our use case, ALSTOM proposed an out-of-context safety control system conforming to SIL4 EN 50129:2018 based on a minimal set of functional safety COTS as a platform. In this use case, model checking, and mutation testing are tested to achieve high levels of THR/TFRR. Railway control systems traditionally are multi-tier fully hierarchical, and ALSTOM generic out-of-context platform is potentially applicable at any of its levels. To exercise and test the feasibility of this concept, we use a simplified BLDC motor controller with safety communications and execution under a 2oo2 architecture. The ambition is to use all elements of real-world railway-related safety control, such as the operation of actuators, sensor acquisition, data processing, and computing as well as communication, all under the premises of railway safety.

Railway hierarchical control system

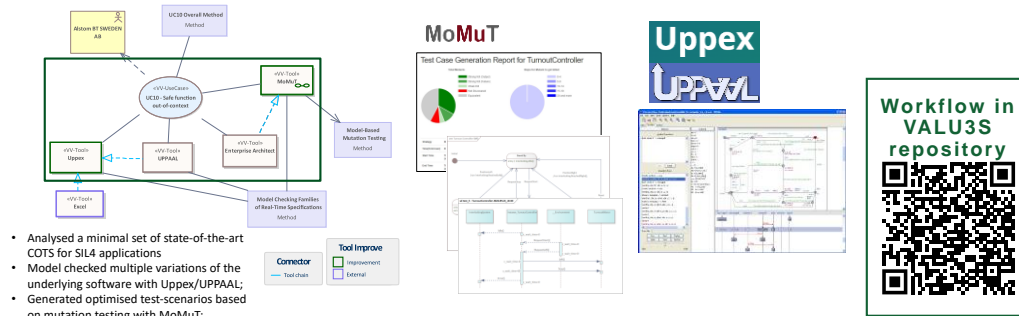


Demonstrator overview



### Connection of the tool(s)

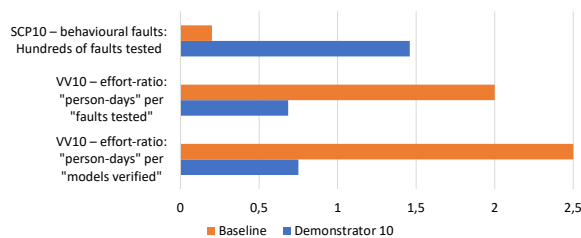
The tool workflow support the verification and validation of safety function in signalling railway applications



- Analysed a minimal set of state-of-the-art COTS for SIL4 applications
- Model checked multiple variations of the underlying software with Uppex/UPPAAL;
- Generated optimised test-scenarios based on mutation testing with MoMuT;

### Evaluation

This demonstrator was evaluated with respect to the number of software faults that are tested (SCP10, where more is better), the effort (time \* person) for each fault tested (VV10, where less is better), and the effort for each property and model formally verified (VV10, where less is better).



### Expected Impacts

- Reducing number of design and implementation errors
- Reducing production cost and effort
- Minimizing energy consumption

### Related/ Impacted Standards

- EN 50126: Generic RAMS process in railway control
- EN 50128: Software for programmable electronic systems for use in railway control and protection applications
- EN 50129: Safety related electronic systems for signalling
- IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related System

### Involved VALU3S Partners

Leader: **ALSTOM** Participating Partners: **AIT** (Austrian Institute of Technology), **isep** (Instituto Superior de Engenharia do Porto), **P.PORTO**, **LieberLieber**

VALU3S HAS RECEIVED FUNDING FROM THE ECSEL JOINT UNDERTAKING UNDER GRANT AGREEMENT NO 876852. THE JOINT UNDERTAKING RECEIVES SUPPORT FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME AND AUSTRIA, CZECH REPUBLIC, GERMANY, IRELAND, ITALY, PORTUGAL, SPAIN, SWEDEN, TURKEY.

**ECSEL Joint Undertaking**  
Electronic Components and Systems for European Leadership



## A.11 Use Case 11



**Developed in Use Case 11 –  
Automated Robot Inspection  
Cell for Quality Control of  
Automotive Body-in-White**



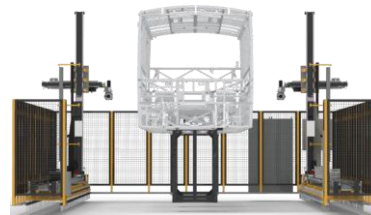
# V&V of an Automated Robot Inspection Cell for Automotive Body-In-White

### Description of Demonstrator

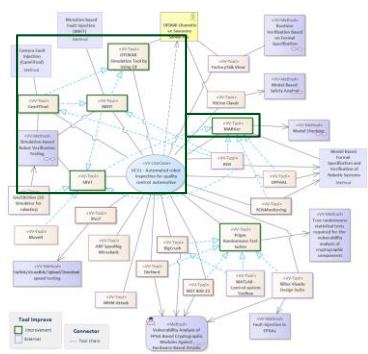
The targeted use case focuses on a novel system using new visual inspection techniques to shorten the duration of existence control of the vehicles' parts for better automotive body-in-white inspection. The baseline of this use case is to provide a better fault-tolerant production system to achieve better quality control. Control of the existence of 2500–3000 body parts is executed fully automatically by a cartesian robot and camera sensor system. This demonstration is a unique and typical application of V&V in automotive production life cycle. This demonstration aims to present the following concrete scenarios over a simulation environment and also the presentation of the physical environment with a table-top model of the inspection system installed in Otokar's premises:

**Scenario 1-** Execution of the inspection system according to the predefined safety trajectory and secure end-to-end quality inspection

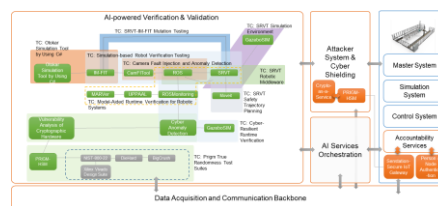
**Scenario 2-** Anomaly and attack detection by considering the corner cases like cyber-attacks, mutation-based software fault injection, identification of the faulty images, vulnerability analysis of cryptographic components.



### Connection of the tool(s)



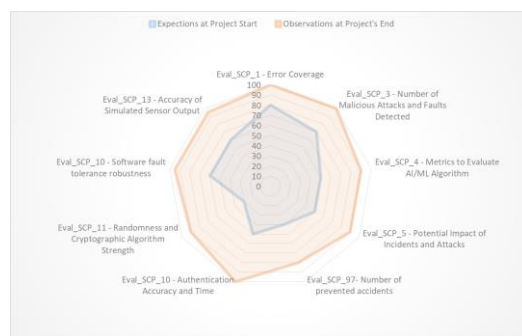
- Tailored Mutation-based Fault Injection Tool (IM-FIT)
- Camera Fault Injection Tool (CamFITTool)
- Simulation-based Robot Verification Tool (SRVT)
- Model-Aided Runtime Verification for Robotic Systems (MARVer)
- Prigm Randomness Test Suites



**Workflow in VALU3S repository**

### Evaluation

Coverage (%) of results adopted by the Industry (Otokar)



**10**

Toolchains Validated in

**2**

Environments (Otokar Sakarya Premises & ESOGU IFARLAB) with

**5**

Novel HW/SW V&V Tools

### Expected Impacts

- State of the art system in the Safety, Cybersecurity, Privacy.
- End-to-end integration of data in the network and verification that it is encrypted.
- Better quality and control with less time and cost.
- Existence control of minimum %95 parts of vehicle in less than 25 minutes.

### Related/ Impacted Standards

- **ISO/IEC 27002:2013:** Information technology — Security techniques — Code of practice for information security controls
- **EN ISO 13849-1:** Safety of machinery. Safety-related parts of control systems General principles for design
- **EN/IEC 62061:** Safety of machinery - Functional safety of safety-related electrical, Electronic and programmable electronic control systems
- **ISO 10218-12:** Robots and robotic devices — Safety requirements for industrial robots
- **ISO/TS 15066:** Specifies safety requirements for collaborative industrial robot systems

### Involved VALU3S Partners

Leader: **Otokar**

Participating Partners:



VALU3S HAS RECEIVED FUNDING FROM THE ECSEL JOINT UNDERTAKING UNDER GRANT AGREEMENT NO 876852. THE JOINT UNDERTAKING RECEIVES SUPPORT FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME AND AUSTRIA, CZECH REPUBLIC, GERMANY, IRELAND, ITALY, PORTUGAL, SPAIN, SWEDEN, TURKEY.



## A.12 Use Case 13



Developed in Use Case 13 – Industrial Drives for Motion Control



# Real-Time Analogue Signal Monitoring (RTAMT) for a Digital Twin for Motion Control

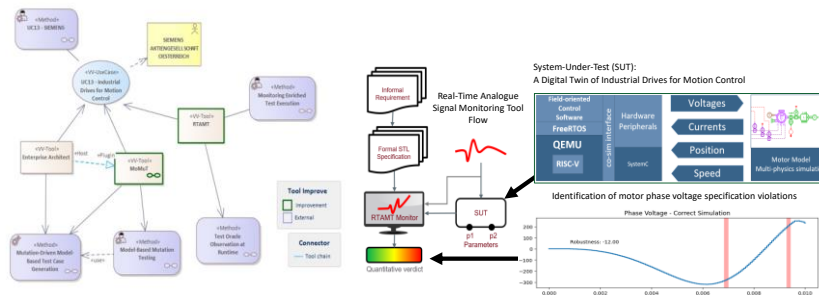
### Description of Demonstrator

In this demonstrator, the use of method "Fault Localization for Specification-based real-time monitoring" in the digital twin for motion control is shown. The digital twin comprises a Permanent Magnetic Synchronous Motor (PMSM), which is modelled in simulation tool AMESim, interfaced to hardware peripherals implemented with SystemC, and a RISC-V-based QEMU. RTAMT is a runtime verification library, developed by AIT and written in Python under the liberal BSD-3 license. RTAMT takes a simulation measurement and a requirement formalized in Signal Temporal Logic (STL) to evaluate robustness degree, which indicates how well the observed behaviour satisfies or how badly it violates the requirement. In this demonstrator, analogue signals such as motor phase voltages from AMESim are used to generate faulty simulation data. This data is then checked against the formally defined requirements. The graphical results generated by RTAMT help to identify faults areas quickly and increase verification quality.



### Connection of the tool(s)

The RTAMT (Real-Time Analogue Signal Monitoring) tool supervises motor signals of a Motion Control Digital Twin application.

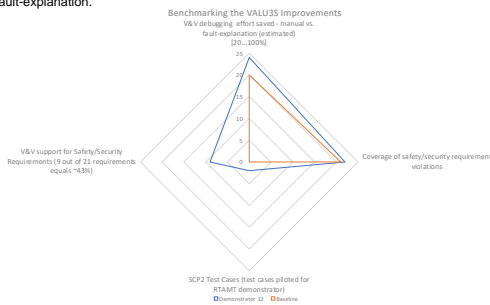


Workflow in VALU3S repository



### Evaluation

The analogue signal monitoring technique supports 43% of safety/security requirements for V&V activities in UC13. The detection of safety/security violations could also be covered by other methods. However, this approach increased verification quality by the introduction of fault-explanation.



### Expected Impacts

- Faster verification process (support for bug/fault analysis) enabled by fault-explanation method (visualization of specification violations)
- Reduced verification environment development efforts due to automatically generated signal monitors for verification
- Support for system optimization (tighter/looser specification for signals) due to fault-explanation
- Reduced verification costs due to open-source tool (no license fees)
- The application of signal monitors can increase verification quality because it can reveal design flaws in the Design-under-Test (model and simulation setup).

### Related Standards

- IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related System

### Involved VALU3S Partners

Leader: **SIEMENS**

Participating Partners:




VALU3S HAS RECEIVED FUNDING FROM THE ECSEL JOINT UNDERTAKING UNDER GRANT AGREEMENT NO 876852. THE JOINT UNDERTAKING RECEIVES SUPPORT FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME AND AUSTRIA, CZECH REPUBLIC, GERMANY, IRELAND, ITALY, PORTUGAL, SPAIN, SWEDEN, TURKEY.






## A.13 Use Case 14








Developed in Use Case 14 –  
CardioWheel



# Instrumented Driving Simulator for Drowsiness Data Generation

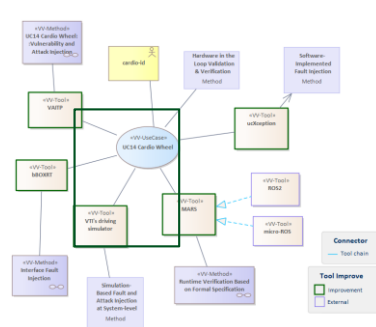
### Description of Demonstrator

Two VTI's driving simulators were equipped with CardioWheels to conduct drowsy driver data collection. **On human-factor-based ML systems, data quality and quantity are of the utmost importance to guarantee reliable predictions.**

-  Sweden, VTI's Facilities
-  20 Participants (10 Female)  
Age 20-60yrs
-  Passenger Vehicle Driving License  
Regular Driving
-  Sleep Disorders  
Motion Sickness  
BMI > 35
-  EGG  
EOG  
Reaction Times  
KSS Scores



### Connection of the tool(s)

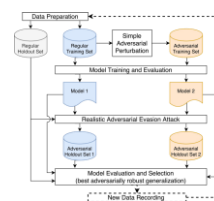


- VTI's Driving Simulator provides data acquisition capabilities
- Extension of VTI's Driving Simulator to collect Reaction Time (RT)
- Application of Robust Adversarial Data to create ML models resilient against faulty input data

### VTI's Driving Simulator

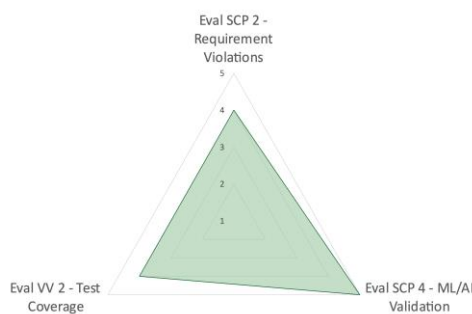


Workflow in VALU3S repository



### Evaluation

Robust Adversarial Training was applied to drowsiness datasets with the same structure, as well as several model designs, testing their baseline performance and the increased model resilience against faulty data.



### Expected Impacts

- Data set collected can be used to properly test driver drowsiness models.
- Validation of Reaction Time as a drowsiness metric can ease the extension of training datasets for this model.
- Robust adversarial training applied to these models reveals increased model robustness against faulty data readings.

### Related/ Impacted Standards

No standardisation work within this demonstrator

### Involved VALU3S Partners

Leader: 

Participating Partners:



VALU3S HAS RECEIVED FUNDING FROM THE ECSEL JOINT UNDERTAKING UNDER GRANT AGREEMENT NO 876852. THE JOINT UNDERTAKING RECEIVES SUPPORT FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME AND AUSTRIA, CZECH REPUBLIC, GERMANY, IRELAND, ITALY, PORTUGAL, SPAIN, SWEDEN, TURKEY.





Developed in Use Case 14 – CardioWheel



# Hardware-in-the-Loop Validation Station

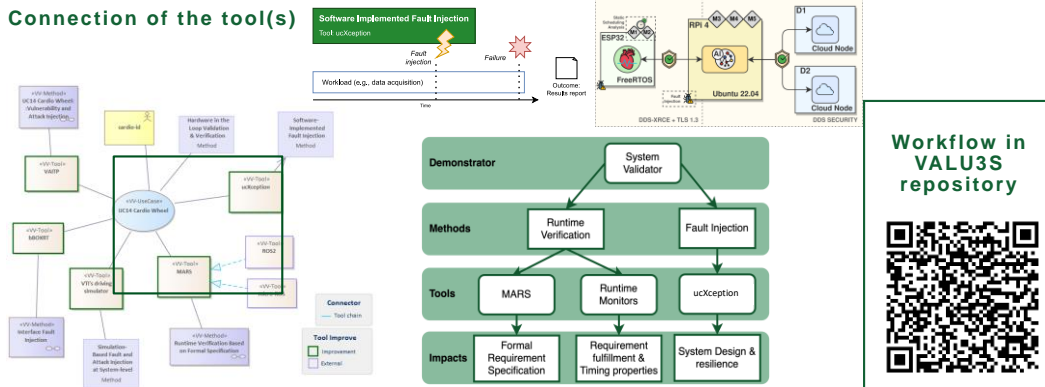
## Description of Demonstrator

This demonstrator shows the result of combining runtime verification and fault injection methods into an automated full-system validation setup.

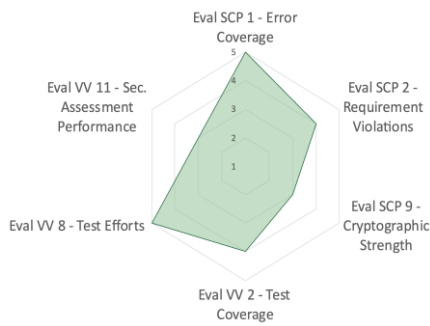
- Defines system requirements as formal statements verifiable by software monitors
- Implements software-based fault injection
- Hides several steps of rigorous system validation behind a simple-to-use interface, greatly reducing the time, cost, and expertise needed to run it, all while increasing our confidence in deployed units.



## Connection of the tool(s)



## Evaluation



Simple test modules are managed by the station's central unit:

- This evaluation is measured with single test runs that isolate components measurement.
- Modules can be combined to create complete validation workflows for different device versions and configurations.

## Expected Impacts

- Improved and streamlined V&V processes for embedded system development
- Robust verification process for continuous development of ML models.
- Strengthened cybersecurity and privacy
- Automatized steps in V&V process.

## Related/ Impacted Standards

No standardisation work within this demonstrator

## Involved VALU3S Partners

Leader:

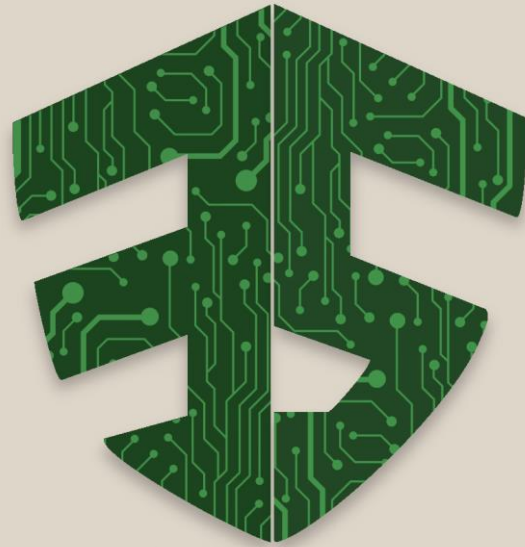
Participants:

VALU3S HAS RECEIVED FUNDING FROM THE ECSEL JOINT UNDERTAKING UNDER GRANT AGREEMENT NO 876852. THE JOINT UNDERTAKING RECEIVES SUPPORT FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME AND AUSTRIA, CZECH REPUBLIC, GERMANY, IRELAND, ITALY, PORTUGAL, SPAIN, SWEDEN, TURKEY.

ECSEL Joint Undertaking  
Electronic Components and Systems for European Leadership

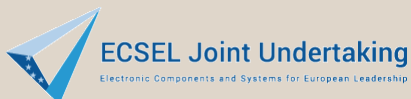






VALU3S

[www.valu3s.eu](http://www.valu3s.eu)



This 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.