Verification and Validation of Automated Systems' Safety and Security

VALU3S

About the Project

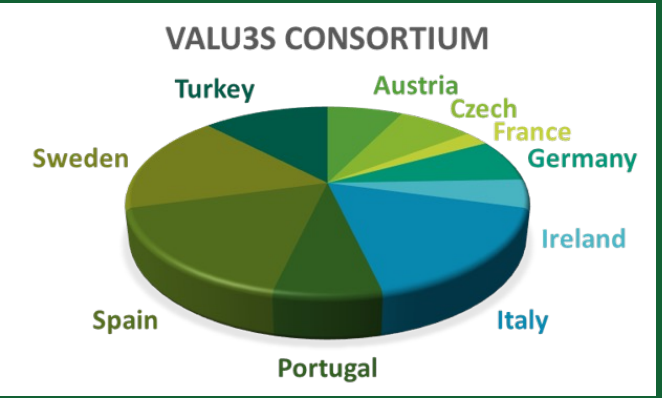
The high complexity of an automated system incurs overhead on the Verification and Validation process, making it time-consuming and costly.

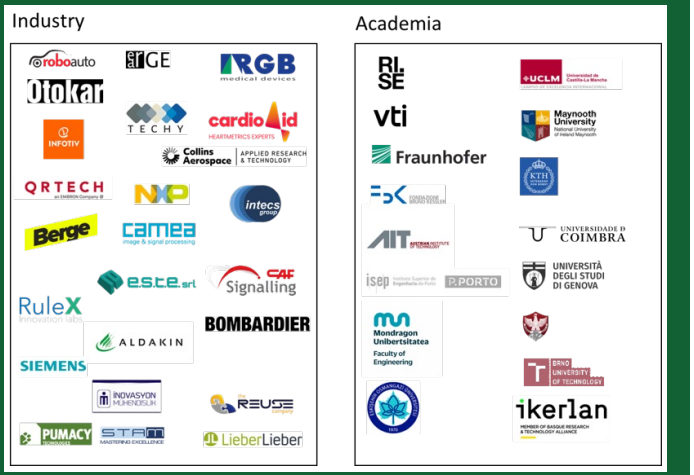
VALU3S aimed to design, implement and evaluate state-of-the-art Verification and Validation methods and tools that reduce the time and cost needed to verify and validate automated systems with respect to safety, cybersecurity and privacy requirements.

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 €.



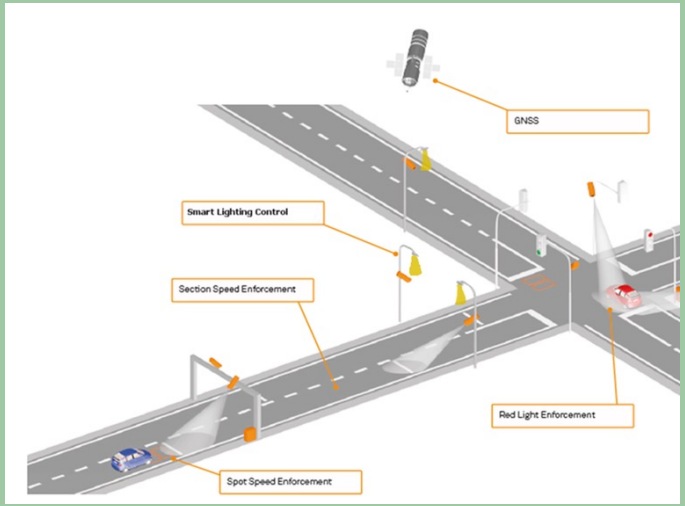


Demonstrations of UC1 - Intelligent Traffic Surveillance

VALU3S

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.



Missions of the lead demonstrators

- Radar/camera-advanced detection and tracking system uses ML component(s), which are 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 System Using Traffic Simulator
2) Testing network communication using NetLoiter

UC1 in the web repository

V&V of Vehicle LP Detection System Using Traffic Simulator

This demo showcases a photo-realistic Berge Simulator to model traffic scenarios for V&V of the CAMEA ML-based LP recognition system.

The system is 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

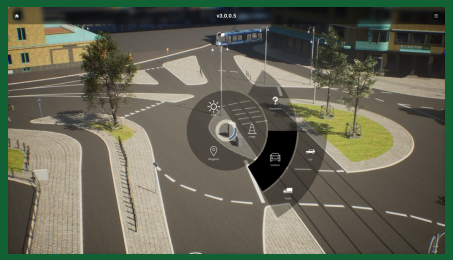
Contact person for the demo

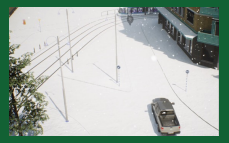
Joakim Rosell
(joakim.rosell@ri.se)

Impressions

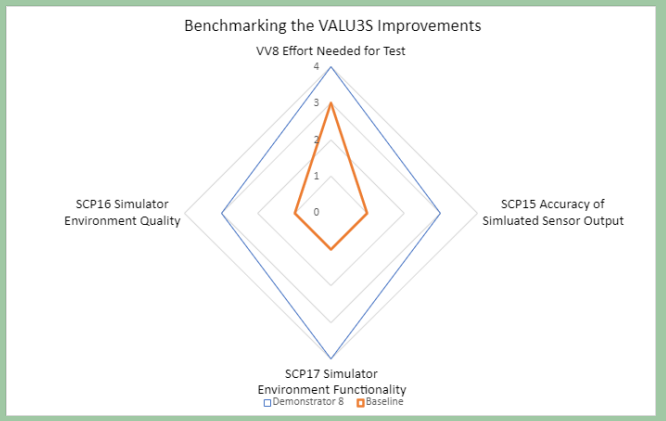
Real image of "Åkareplatsen resecentrum" in Gothenburg, Sweden and corresponding synthetic scene generated in the Berge simulator.

Example images from the Berge simulator with configurable scenario parameters





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

Testing network communication using 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.

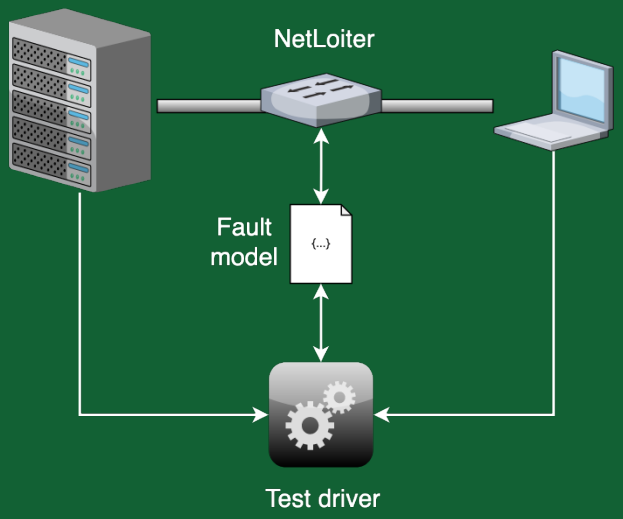
Link to demo pitch video

Contact person for the demo

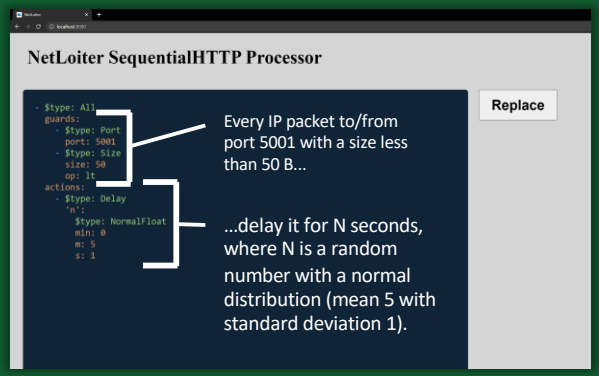
Ales Smrcka
(smrcka@vutbr.cz)

Impressions

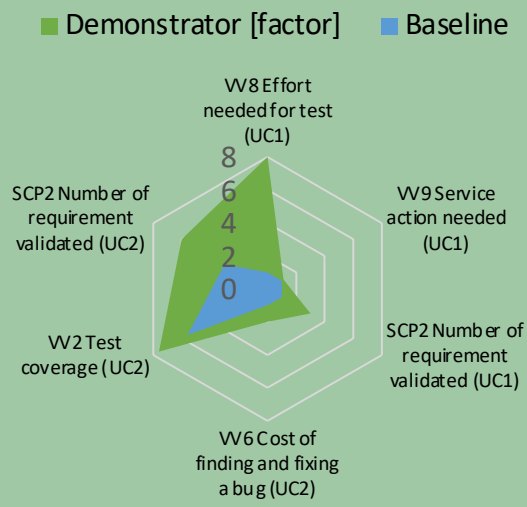
Scheme of the NetLoiter intercepting the connection between two computers or IoT devices.



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



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

BRNO UNIVERSITY OF TECHNOLOGY

camea

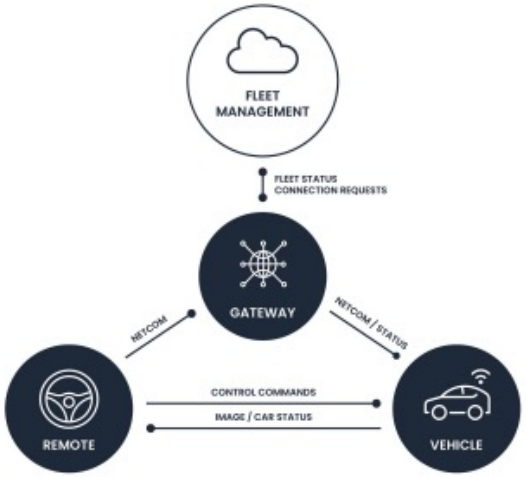
roboauto

Demonstrators of Use Case 2 - Car Teleoperation

VALU3S

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.



Missions of 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

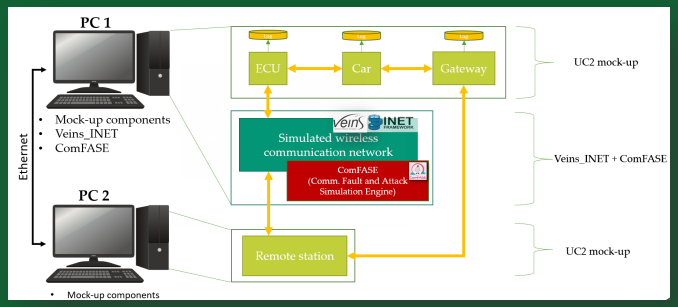
Contact person for the demo

Mateen Malik
(mateen.malik@ri.se)

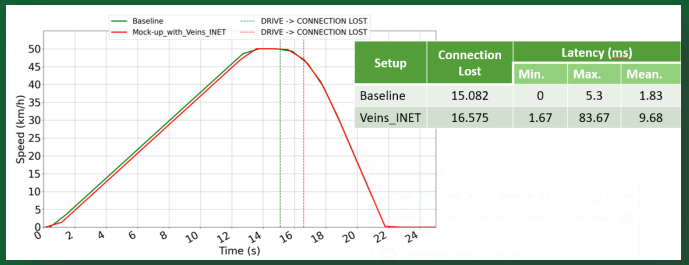
Impressions

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

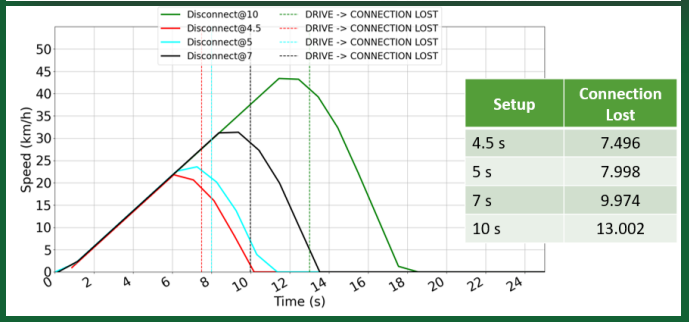
UC2 Demonstrator Implementation with Simulated Network



Simulation Resuls

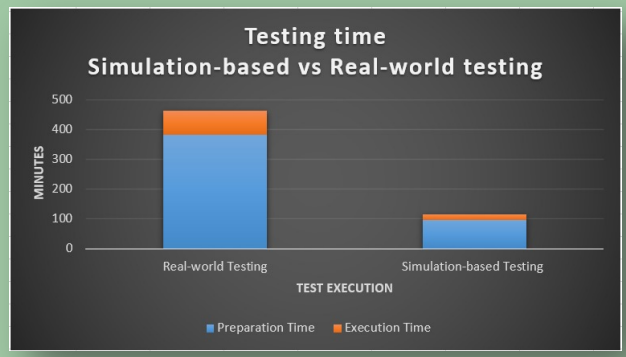


Setup	Connection Lost	Latency (ms)		
		Min.	Max.	Mean.
Baseline	15.082	0	5.3	1.83
Veins_INET	16.575	1.67	83.67	9.68



Setup	Connection Lost
4.5 s	7.496
5 s	7.998
7 s	9.974
10 s	13.002

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

RI SE roboauto vti

Demonstrators of Use Case 3 - Radar System for ASAS

VALU3S

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.

Missions of the lead demonstrators

- Validation ends after unit testing, and thus, radar system bugs are often detected late. Thus, system testing will be enabled at IC supplier level
- Resolve the 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 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.

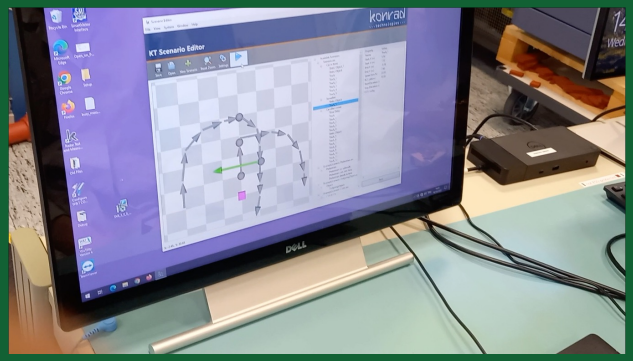
Link to demo pitch video

Contact person for the demo

Manuel Schmidt
(manuel.Schmidt@nxp.com)

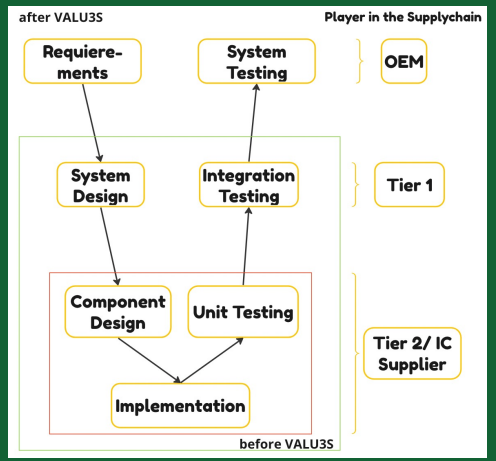
Impressions

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

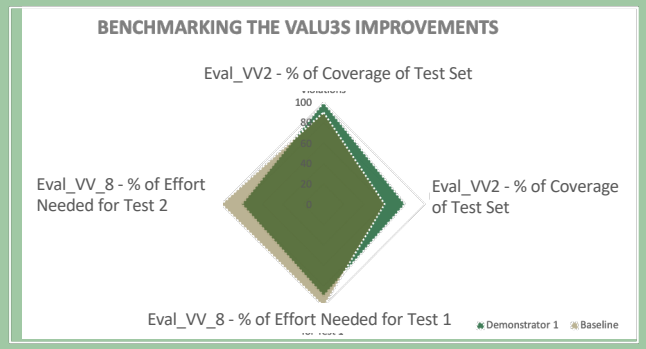


HW set up inluding a whole radar system producing a radar point cloud from the simulated scenario

The simualtion 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

Demonstrators of Use Case 4 - Human-Robot-Interaction in Semi-Automatic Assembly Processes

VALU3S

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.

Mission of 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 gripper of the robot without 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)

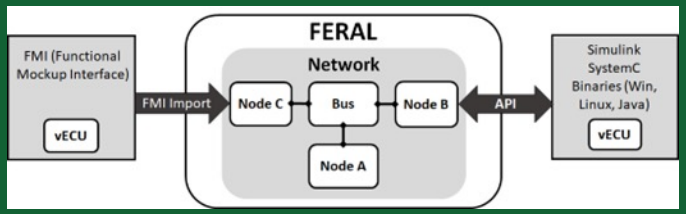
Link to demo pitch video

Contact person for the demo

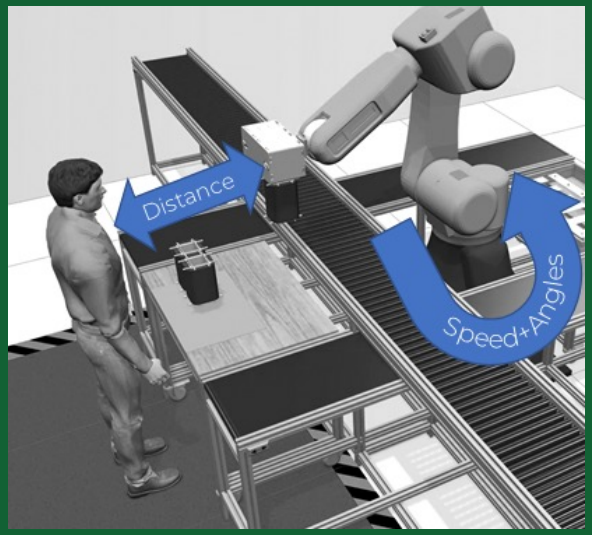
Iron Prandoda Silva
(Iron.PrandodaSilva@iese.fraunhofer.de)

Impressions

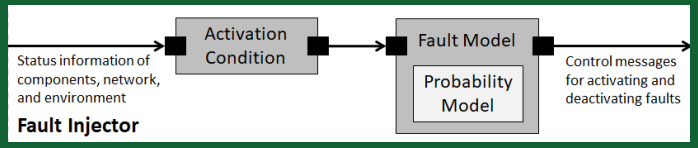
Coupling of different types of simulation models into a holistic simulation scenario



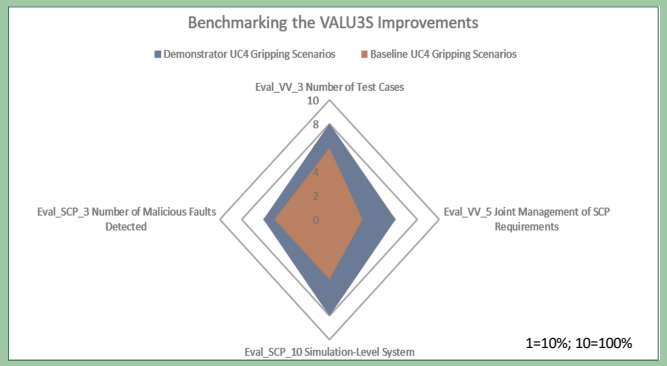
The validation object is a virtual model of the distributed production facility, which contains dedicated virtual models for the production line parts, sensors, and communication networks integrated into a holistic simulation scenario



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



Improvement and Impact



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

PUMACY TECHNOLOGIES

Fraunhofer

UCLM Universidad de Castilla-La Mancha
CAMPUS DE EXCELENCIA INTERNACIONAL

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

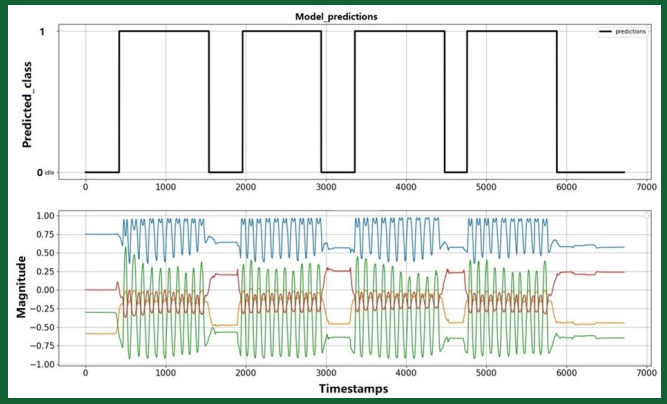
Contact person for the demo

Zain Shahwar
(zain.shahwar@pumacy.de)

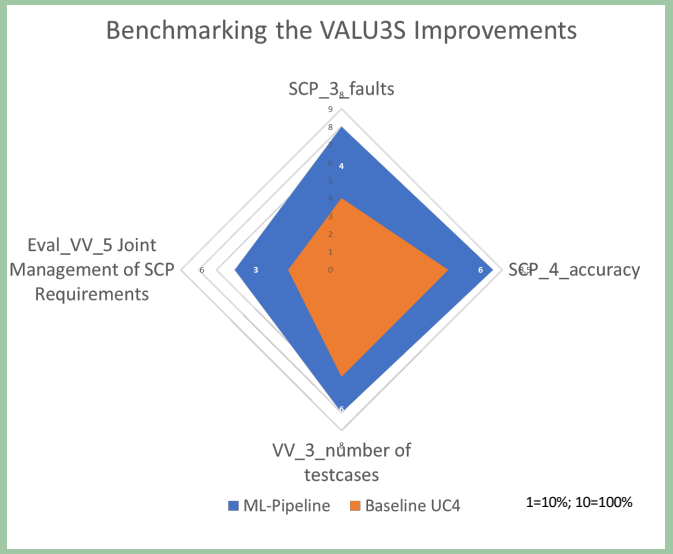
Impressions

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



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

PUMACY TECHNOLOGIES

Fraunhofer

UCLM Universidad de Castilla-La Mancha
CAMPUS DE EXCELENCIA INTERNACIONAL

Virtual & augmented reality-based user interaction V&V

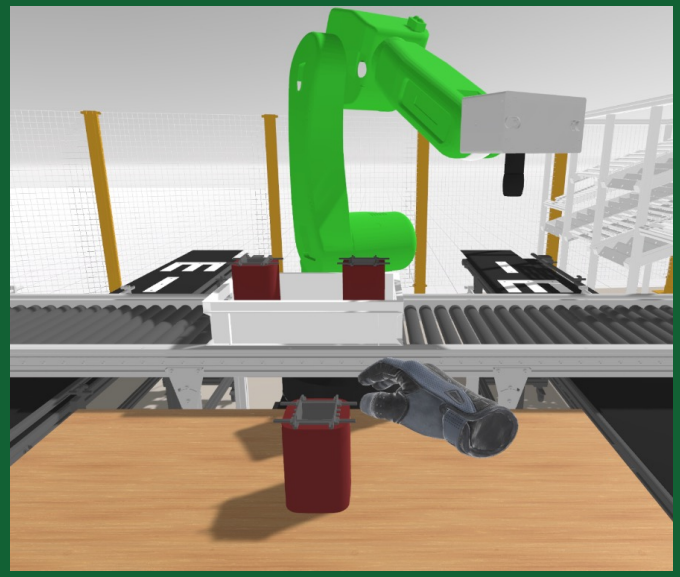
An immersive virtual reality application, namely XR-4-V&V, has been developed to facilitate early human-robot collaboration. This system allows human workers to collaborate with industrial robots in a simulated environment through the use of a head-mounted display. XR-4-V&V is developed using the Unity3D 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, utilising 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 behaviour can be monitored, enabling the analysis of human factors and technology acceptance before the system's full deployment.

Participating partners

PUMACY TECHNOLOGIES

Fraunhofer

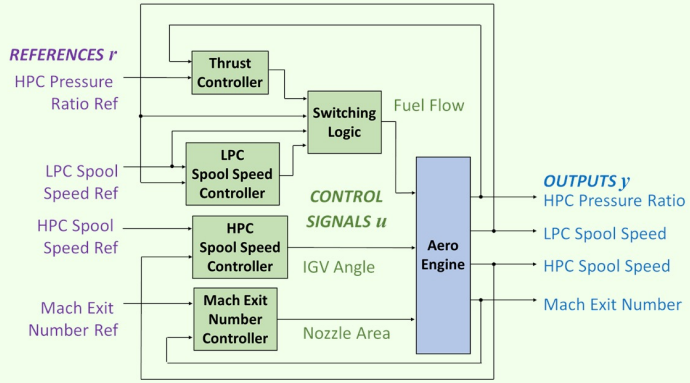
UCLM Universidad de Castilla-La Mancha
CAMPUS DE EXCELENCIA INTERNACIONAL

Demonstrators of Use Case 5 - Aircraft Engine Controller

VALU3S

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.



Missions of 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: synthesizing a robust region (with fixed reference values) and robustness to reference value changes.

Link to demo pitch video

Contact person for the demo

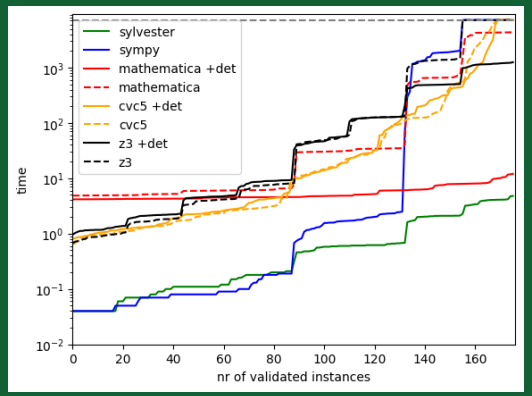
Ludovico Battista
(lbattista@fbk.eu)

Impressions

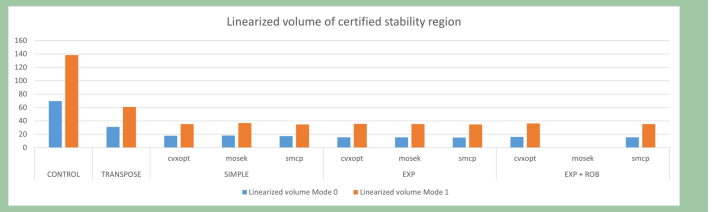
We approach these two targets by use of the tool Sabbath, that is integrated into an ad-hoc script.

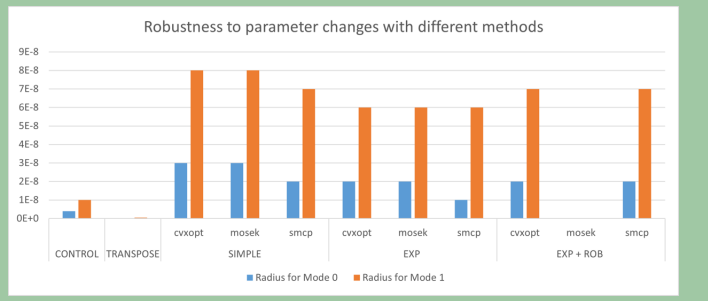
```
Valu3s_demo>python3 verify_po.py --solver z3 --use-exponential --size 5
>> Read matrices
A size 5x5
B size 5x22
C size 4x5
>> Controller matrices
KP1 size 3x4
KP2 size 3x4
KI1 size 3x4
KI2 size 3x4
INFO:__main__:Reference values: [1/2, 5.0, -1.0, 20.0]
INFO:__main__:Finding assumptions...
INFO:__main__:Searching 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 synthesized region of certified stability. Therefore, the total saving depends on the density of the test cases.

Participating partners

CENTER FOR DIGITAL INDUSTRY
FONDAZIONE BRUNO KESSLER

Collins Aerospace

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.

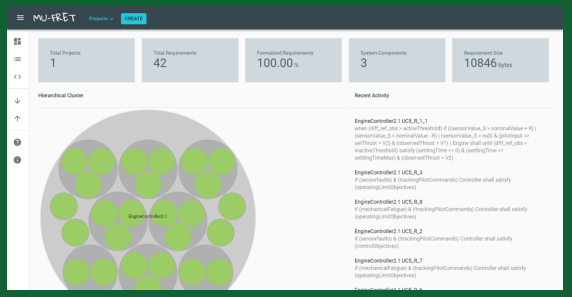
Mu-FRET enables a user to extract parts of a requirement to a new requirement, allowing the extracted part to be reused. Mu-FRET also formally verifies that the refactored requirement (including the extracted parts) has the same behaviour as the original requirement.

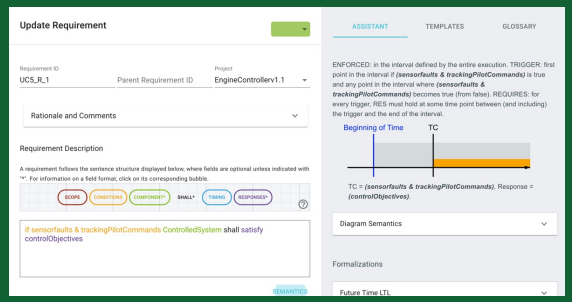
Link to demo pitch video

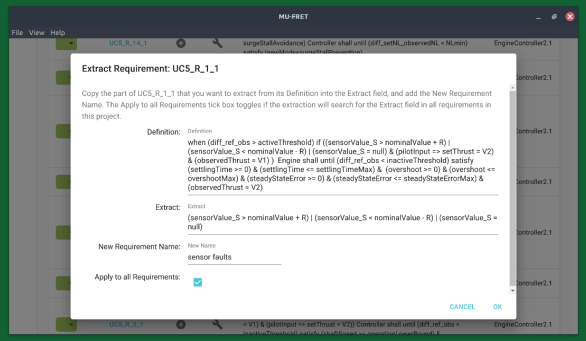
Contact person for the demo
Rosemary Monahan
(Rosemary.Monahan@mu.ie)

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
	Total (Re)Definitions	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

Collins Aerospace

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.

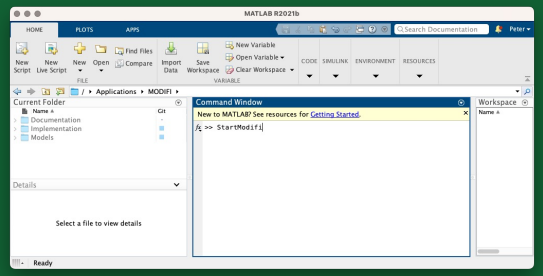
Link to demo pitch video

Contact person for the demo

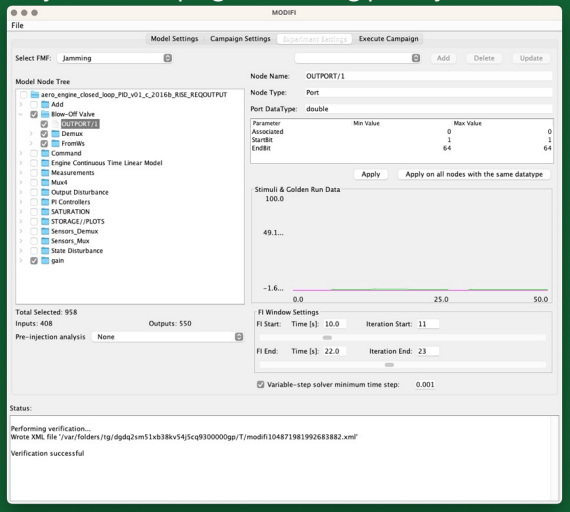
Peter Folkesson
(peter.folkesson@ri.se)

Impressions

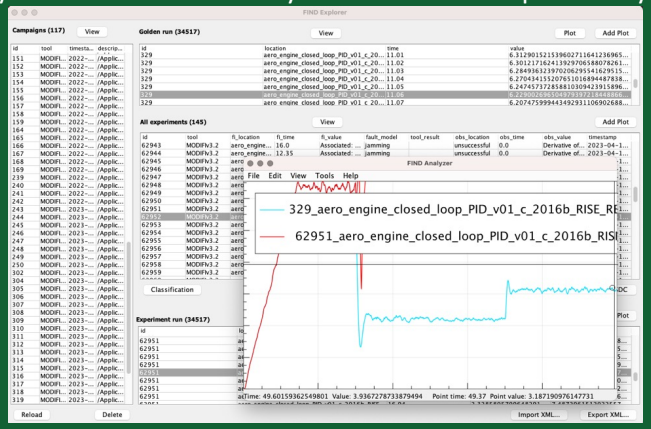
MODIFI is started from the MATLAB command window.



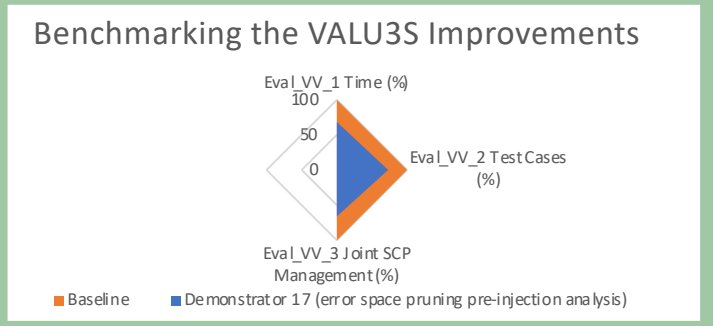
The MODIFI GUI allows configuration and execution of fault/attack injection campaigns including pre-injection analyses.



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



Improvement and Impact



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

RI.SE

Collins Aerospace

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)

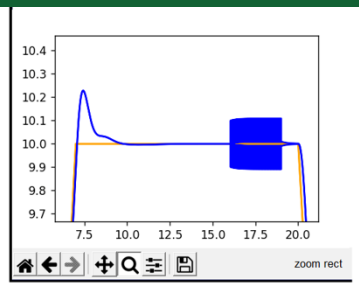
Impressions

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

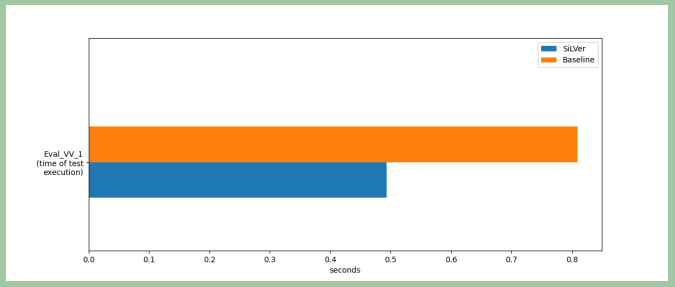
```yaml
system: system.yaml
input-scenarios: input.yaml
output-dir: output

simulation:
  enabled: yes
  type: verification
    # falsification -> typical simulation using floating point quantities
    # verification -> reachability analysis using affine arithmetic

monitoring:
  enabled: yes
  type: 2
    # 1 -> detect changes in reference and measure
    #      quantities of interest in output

    # 2 -> use uncertainty ranges from input and
    #      measure quantities of interest in output

  # desired bounds on measured quantities
  # for requirement satisfaction
  overshoot: 0.1
  settling-time: 4
  steady-state-error: 0.01

  signals: # what should be monitored
    reference: r(3)
    output: y(3)

plotting:
  enabled: yes

  signals: [ # each row corresponds to a separate a plot
    [r(1), y(1)],
    [r(2), y(2)],
    [r(3), y(3)]
  ]
```

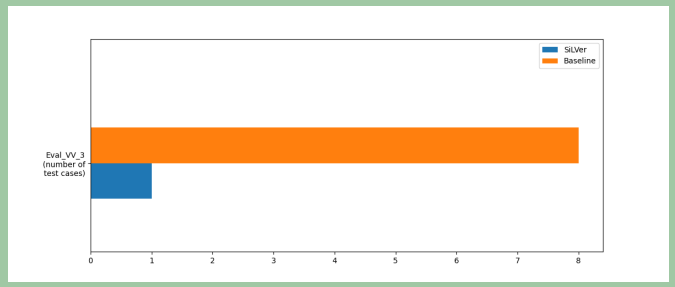
SiLVer output example – includes information about requirement satisfaction and system trajectory plots

```
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

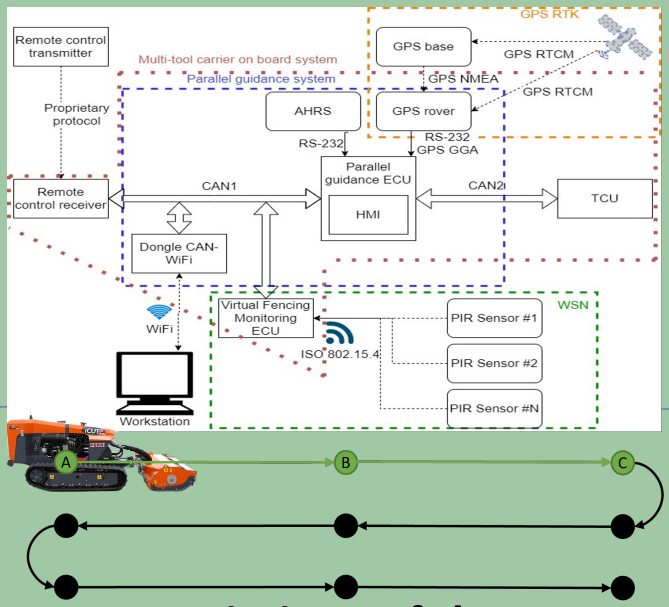
Collins Aerospace

Demonstrators of Use Case 6 - Agricultural Robot

VALU3S

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.



Missions of 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 CHESS-FLA

Demonstration of applying the Model-based Safety Analysis with Failure Logical Analysis (MSA-FLA) method supported by the CHESS-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).

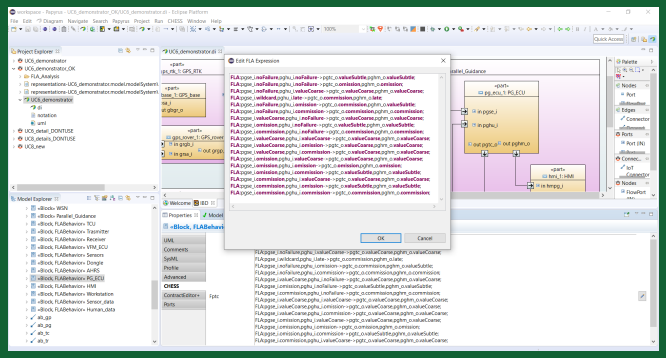
Link to demo pitch video

Contact person for the demo

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

Impressions

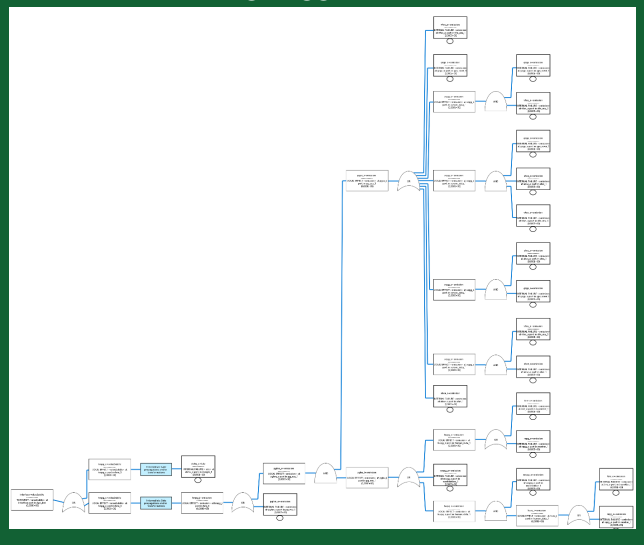
Screen of the CHESS tool with a highlight of the FLA rules of a specific sub-block



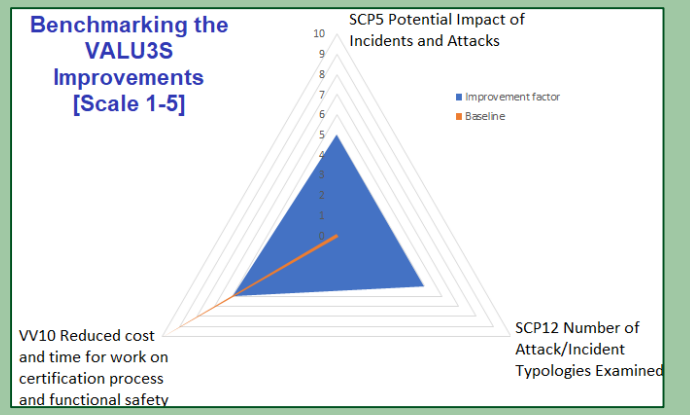
Some FMEA rows automatically generated by the CHESS-FLA tool

SYSTEM PATH	FUNCTION	FAILURE MODES	LOCAL EFFECTS	END EFFECTS	COMPENSATING PROVISION (SAFETY EXPERT)	SEVERITY (SAFETY EXPERT)	FAILURE RATE (SAFETY EXPERT)
Agri_bot.parallel_guidance_1	Dongle_1	(dowo_i.noFailure)	LATE failure at dohu_o port	Agri_bot.movement.valueSubtle			
Agri_bot.parallel_guidance_1	Dongle_1	(dowo_i.noFailure)	LATE failure at dohu_o port	Agri_bot.interface.valueSubtle			
Agri_bot.parallel_guidance_1	Dongle_1	(dowo_i.noFailure)	VALUECOARSE failure at dohu_o port	Agri_bot.movement.valueSubtle			
Agri_bot.parallel_guidance_1	Dongle_1	(dowo_i.noFailure)	VALUECOARSE failure at dohu_o port	Agri_bot.interface.omission			
Agri_bot.parallel_guidance_1	Dongle_1	(dowo_i.omission)	OMISSION failure at dohu_o port	Agri_bot.movement.valueSubtle			
Agri_bot.parallel_guidance_1	Dongle_1	(dowo_i.omission)	OMISSION failure at dohu_o port	Agri_bot.movement.commission			
Agri_bot.parallel_guidance_1	Dongle_1	(dowo_i.omission)	OMISSION failure at dohu_o port	Agri_bot.interface.omission			
Agri_bot.parallel_guidance_1	Dongle_1	(dowo_i.omission)	OMISSION failure at dohu_o port	Agri_bot.interface.valu			

One of the FT automatically generated by CHESS-FLA



Improvement and Impact



The Model-based Safety Analysis with Failure Logical Analysis (MSA-FLA) performed with the CHESS-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

intecs Solutions
the Brainware company

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.

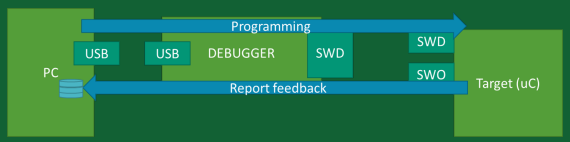
Link to demo pitch video

Contact person for the demo

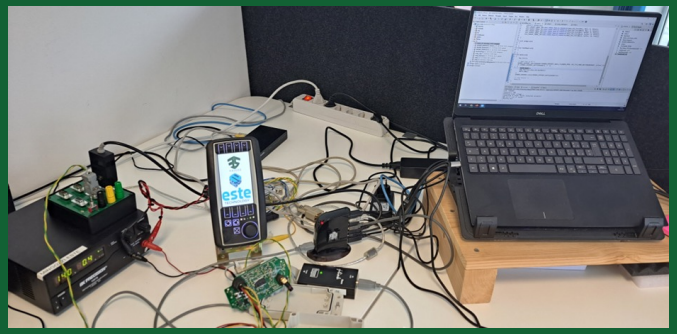
Emanuele Mingozzi
(mingozzi@estetechnology.com)

Impressions

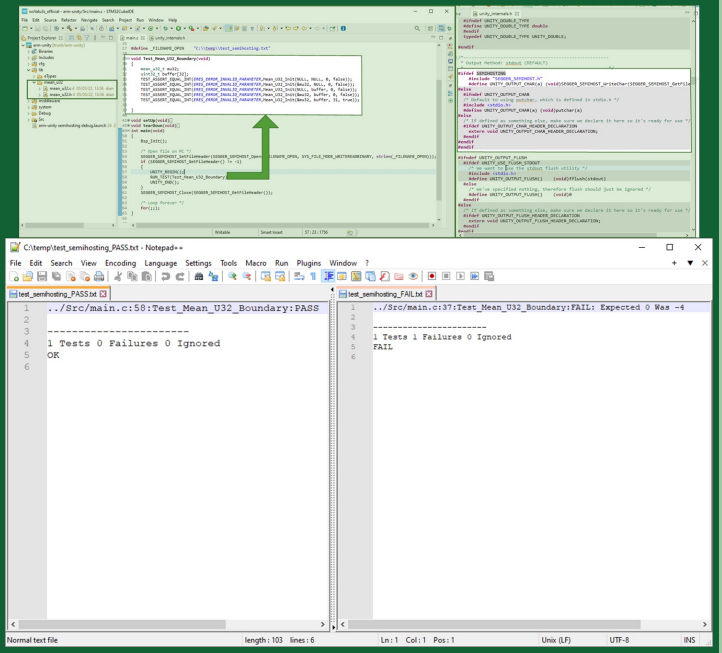
Block diagram of Arm Unity configuration



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.

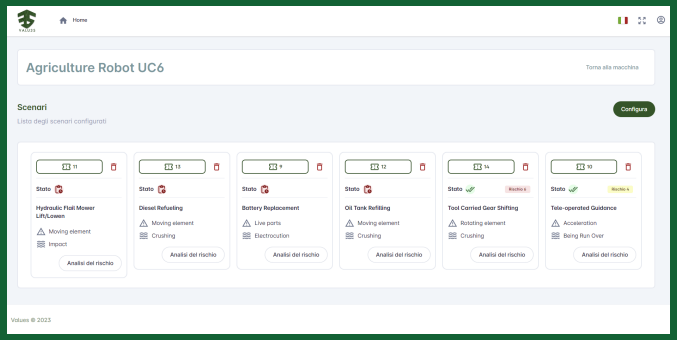
Link to demo pitch video

Contact person for the demo

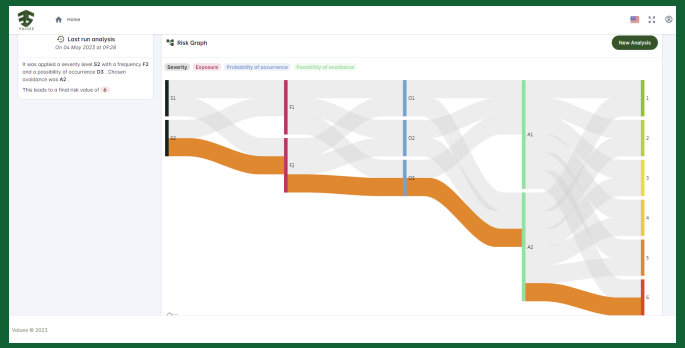
Davide Ottonello
(d.ottonello@stamtech.com)

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.

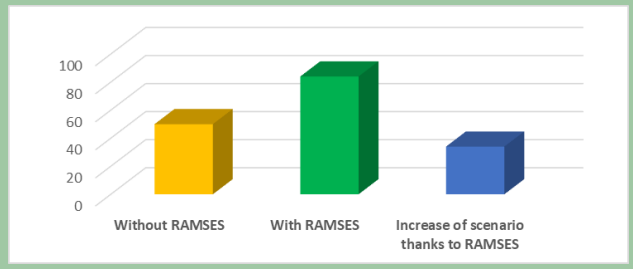


Improvement and Impact

The introduction of RAMSES tool into a state-of-the-art risk management process applied in the use case has lead 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

STAM
MASTERING EXCELLENCE

Demonstrator of Use Case 7

-

Human-Robot Collaboration in a Disassembly Process with Workers with Disabilities

VALU3S

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.

Missions of 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.

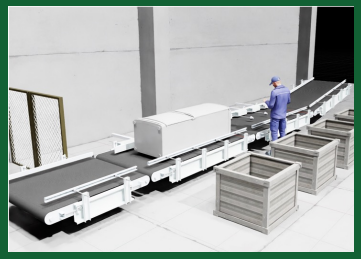
Link to demo pitch video

Contact person for the demo

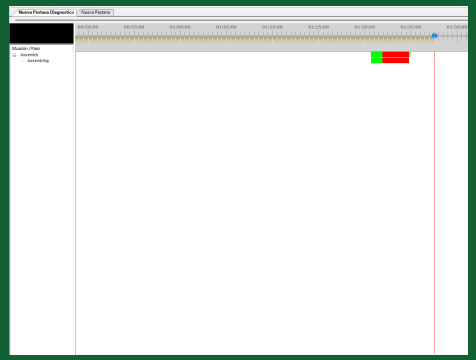
Joseba A. Agirre
(jaagirre@mondragon.edu)

Impressions

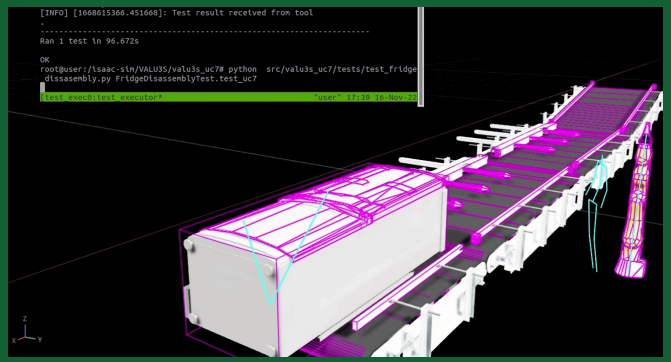
NVIDIA Isaac Sim. Simulation environment for the validation of the human-robot interaction robotic system.



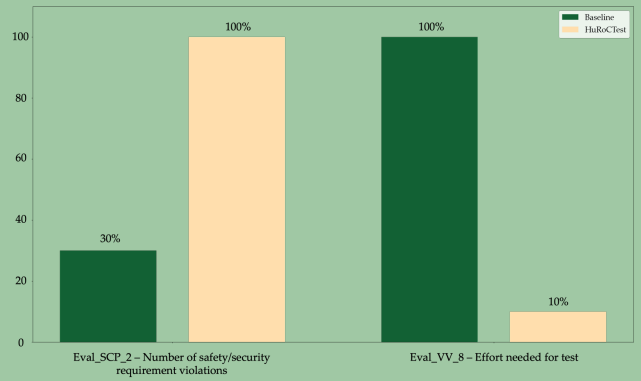
ULISES. Procedural-task evaluation approach for testing simulation-based human-robot interaction.



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

Mondragon Unibertsitatea
Professional Learning Space

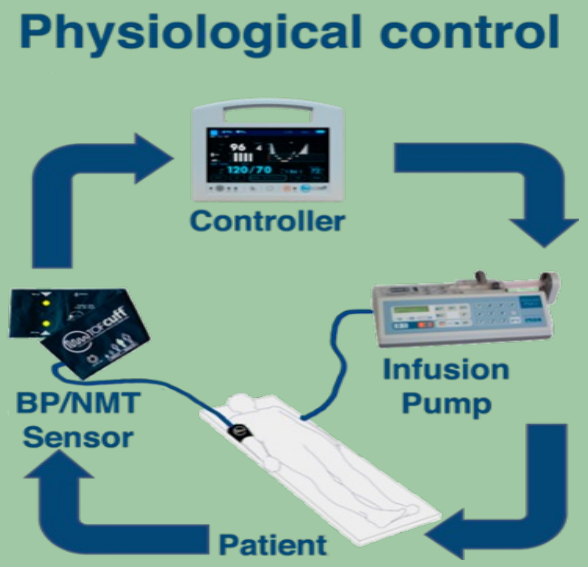
ALDAKIN

Demonstrators of Use Case 8 - NMT Infusion Controller

VALU3S

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.



Missions of the lead demonstrators

Avoid experimental ad 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 CHESS-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.

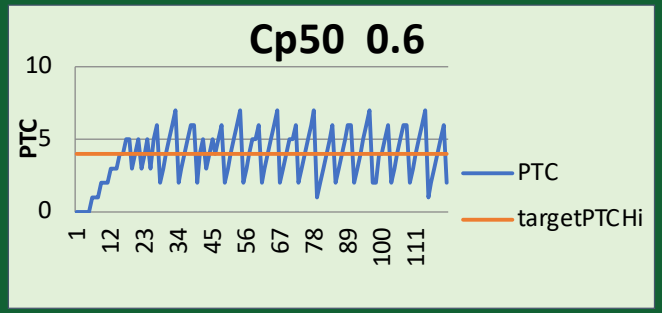
Link to demo pitch video

Contact person for the demo

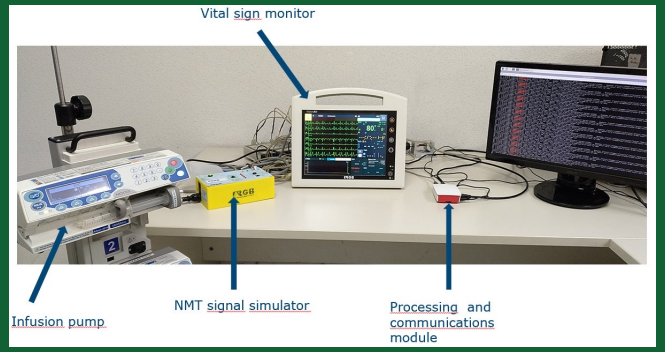
Ricardo Ruiz
(rruiz@rgb-medical.com)

Impressions

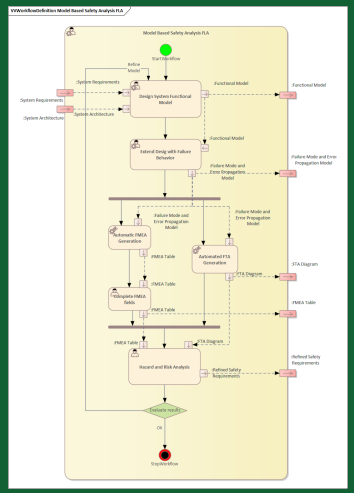
Screen of the NMT Controller results under specific testing conditions.



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

RGB medical devices

BRNO UNIVERSITY OF TECHNOLOGY

MSA-FLA with CHESS-FLA

Demonstration of the application of the Model-based Safety Analysis with Failure Logical Analysis (MSA-FLA) method supported by the CHESS-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).

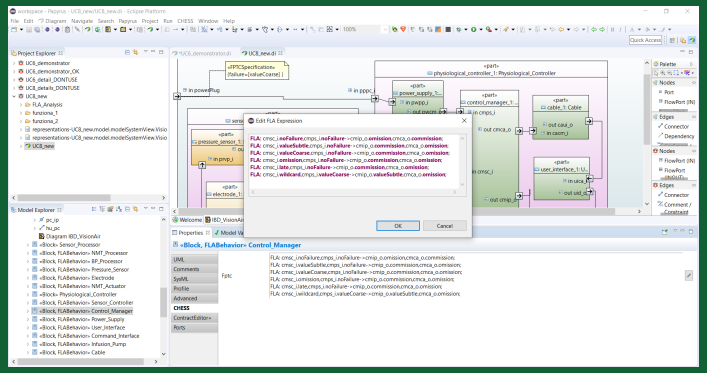
Link to demo pitch video

Contact person for the demo

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

Impressions

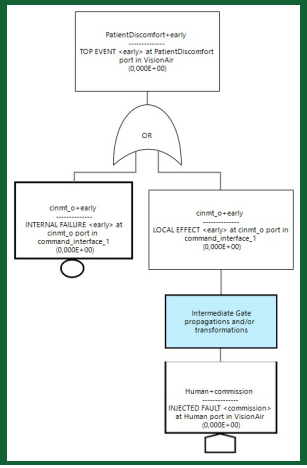
Screen of the CHESS tool with a highlight of the FLA rules of a specific sub-block



Some FMEA rows automatically generated by the CHESS-FLA tool

SYSTEM PATH	FUNCTION	FAILURE MODES	LOCAL EFFECTS	END EFFECTS
VisionAir.physiological_controller_	Controller_manager_1	{cmsc_i.noFailure; cmps_i.noFailure}	OMISSION failure at cmip_o port	VisionAir.ipDiagnostic.omission
VisionAir.physiological_controller_	Controller_manager_1	{cmsc_i.noFailure; cmps_i.noFailure}	OMISSION failure at cmip_o port	VisionAir.ipDiagnostic.valueSubtle
VisionAir.physiological_controller_	Controller_manager_1	{cmsc_i.valueSubtle; cmps_i.noFailure} {cmsc_i.omission; cmps_i.noFailure} {cmsc_i.late; cmps_i.noFailure} {cmsc_i.valueCoarse; cmps_i.noFailure}	COMMISSION failure at cmip_o port	VisionAir.ipDiagnostic.valueSubtle
VisionAir.physiological_controller_	Controller_manager_1	{cmsc_i.valueSubtle; cmps_i.noFailure} {cmsc_i.omission; cmps_i.noFailure} {cmsc_i.late; cmps_i.noFailure} {cmsc_i.valueCoarse; cmps_i.noFailure}	COMMISSION failure at cmip_o port	VisionAir.ipDiagnostic.commission

One of the FT automatically generated by CHESS-FLA



Improvement and Impact

The Model-based Safety Analysis with Failure Logical Analysis (MSA-FLA) performed with the CHESS-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

intecs Solutions
the Brainware company

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

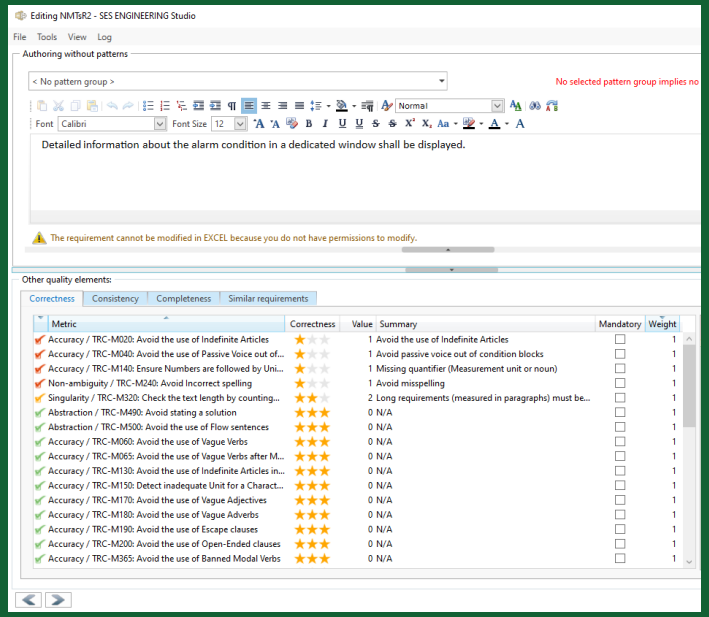
Link to demo pitch video

Contact person for the demo

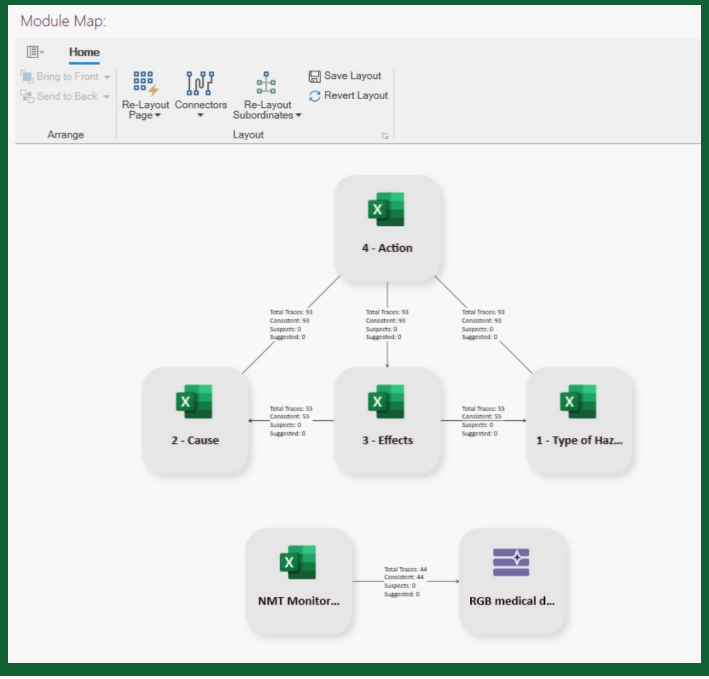
Jose Luis de la Vara
(JoseLuis.delaVara@uclm.es)

Impressions

RQA tool screenshot



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

Demonstrators of Use Case 9 - Autonomous Train Operations

VALU3S

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.

Missions of 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)

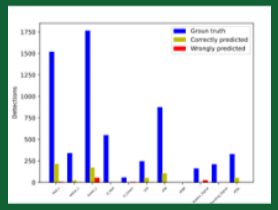
Impressions

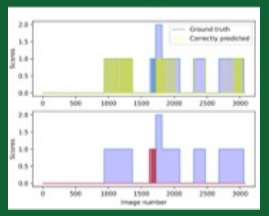
Design of train journey using Train Simulator

Generation of synthetic validation datasets using DaGe4V

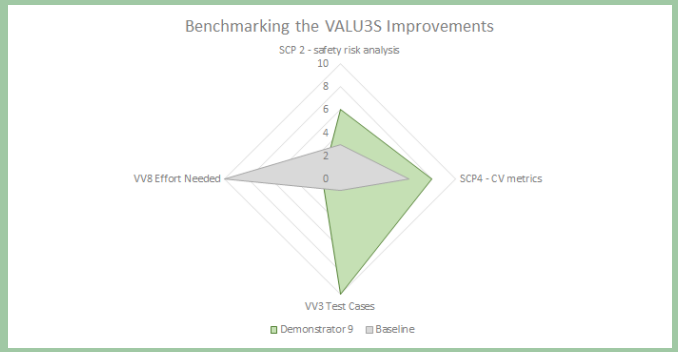
Autumn cloudy morning | Snowy midday | Summer night | Summer afternoon

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

Demonstrators of Use Case 10 - Safety function out-of-context

VALU3S

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.

Missions of 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 VALU3S 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.

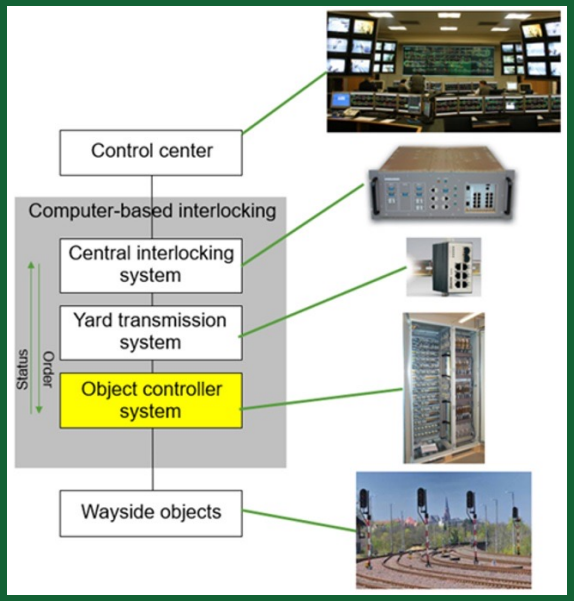
Link to demo pitch video

Contact person for the demo

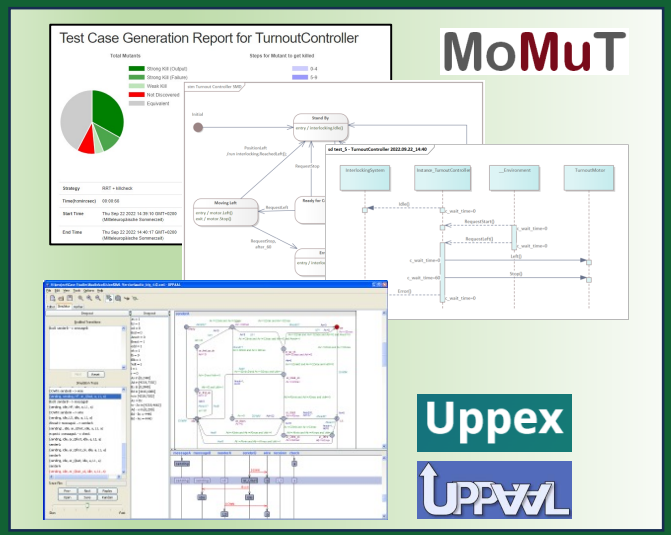
Sina Borrami
(sina.borrami@alstomgroup.com)

Impressions

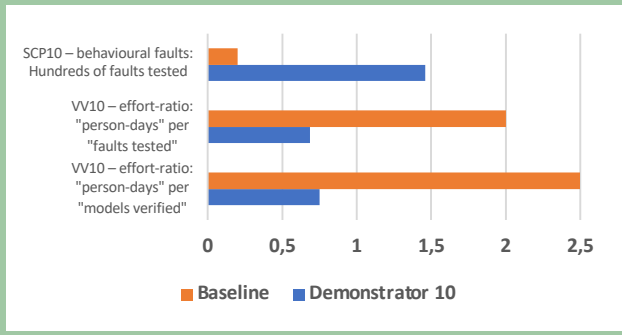
Architecture of the signalling railway system



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

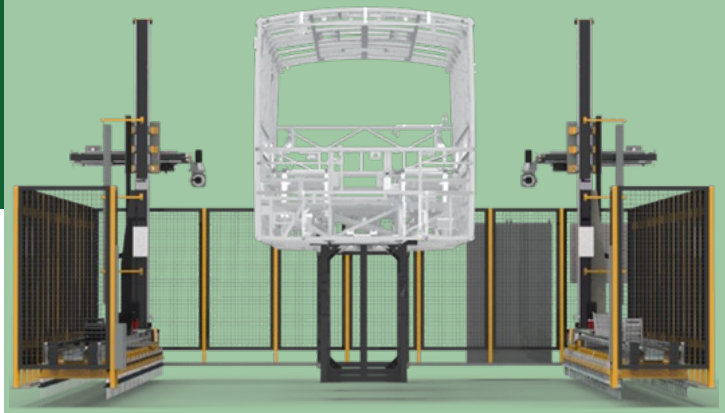
ALSTOM
AIT Austrian Institute of Technology
isep Instituto Superior de Engenharia do Porto
P.PORTO
LieberLieber

Demonstrators of Use Case 11 - V&V of an Automated Robot Inspection Cell for Automotive Body-in-White

VALU3S

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.



Missions of 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 analyze 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

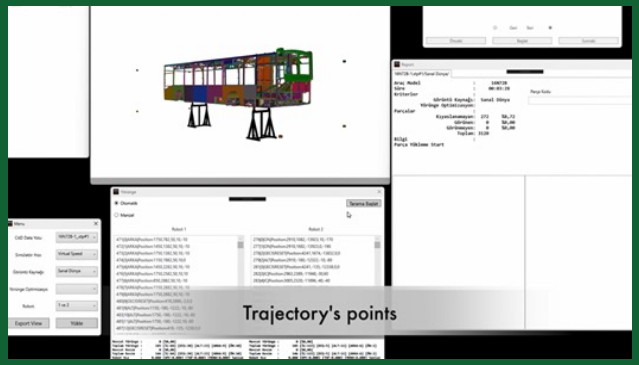
Contact person for the demo

Gürol Çokünlü

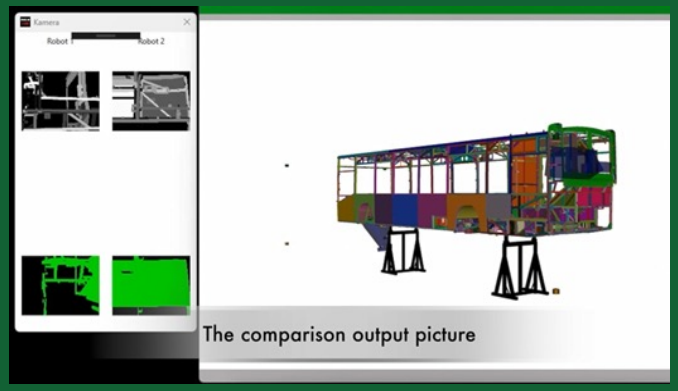
gcokunlu@otokar.com.tr

Impressions

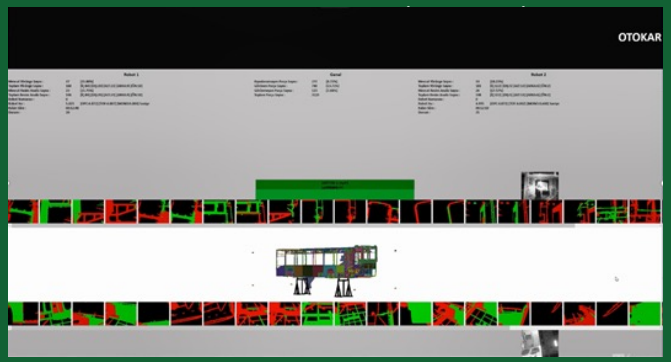
The software in the server side decides trajectory points, than robots start the part existence of vehicle in simulation environment



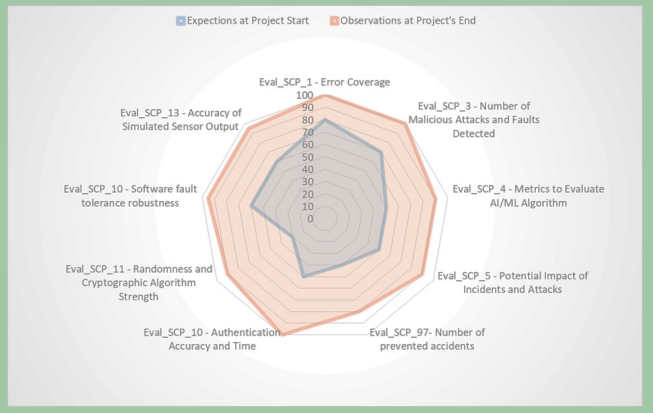
Virtual images which are taken by robots in simulation compares with CAD data of vehicle.



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

Demonstrators of Use Case 13

-

Industrial Drives for Motion Control

VALU3S

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.

Missions of 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. This is addressed by the lead demos.

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.

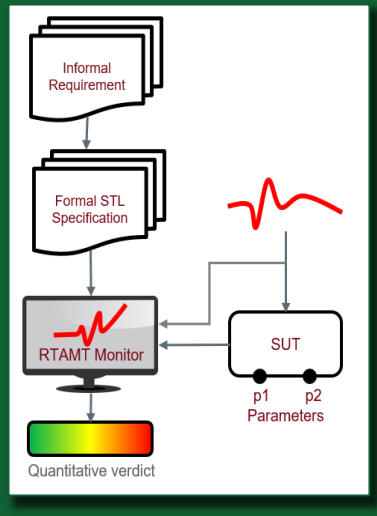
Link to demo pitch video

Contact person for the demo

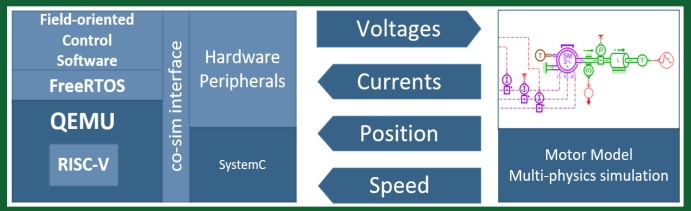
Bernhard Fischer
(bernhard.bf.fischer@siemens.com)

Impressions

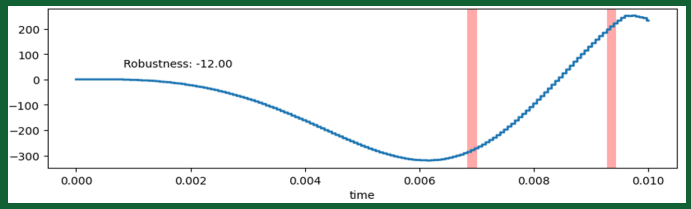
Flow with the Real-Time Analogue Monitoring Tool



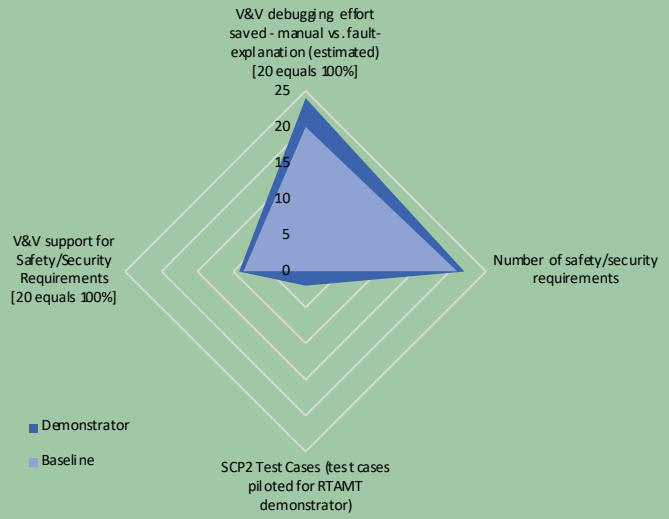
System-Under-Test (SUT): Motion Control Digital Twin built with AMESim, QEMU and SystemC



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

SIEMENS
Fraunhofer
AIT Austrian Institute of Technology
LieberLieber

Demonstrators of Use Case 14

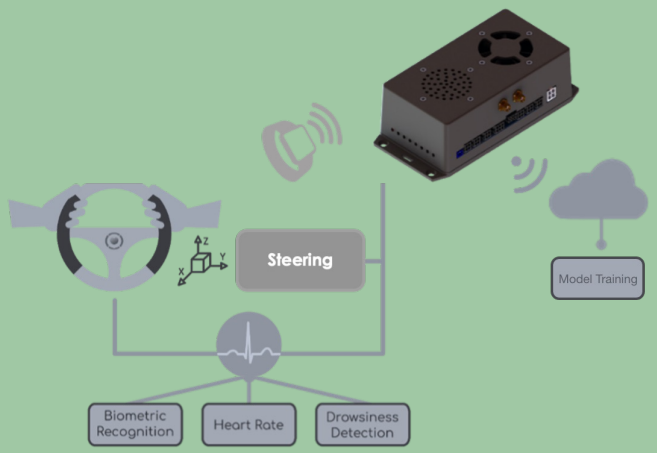
-

CardioWheel

VALU3S

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.



Missions of 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

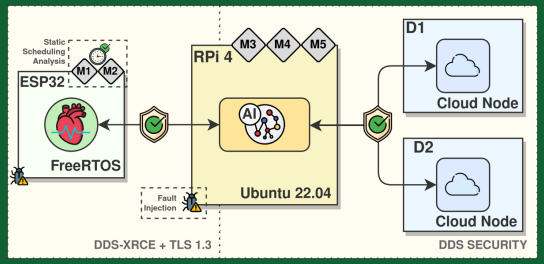
Contact person for the demo

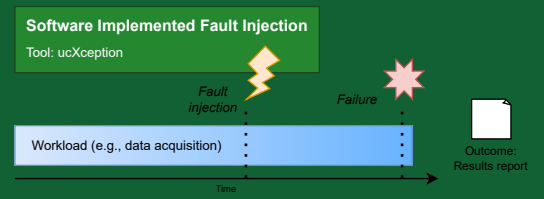
Lourenço Rodrigues (lar@cardio-id.com)

Impressions

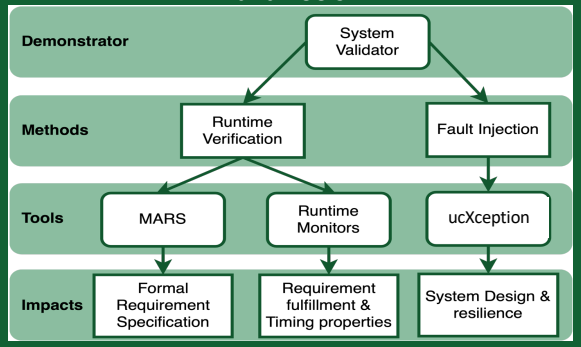
Validation Station with Touch Screen Simple Interface

Monitor generation and fault injected are implemented as formal verification methods

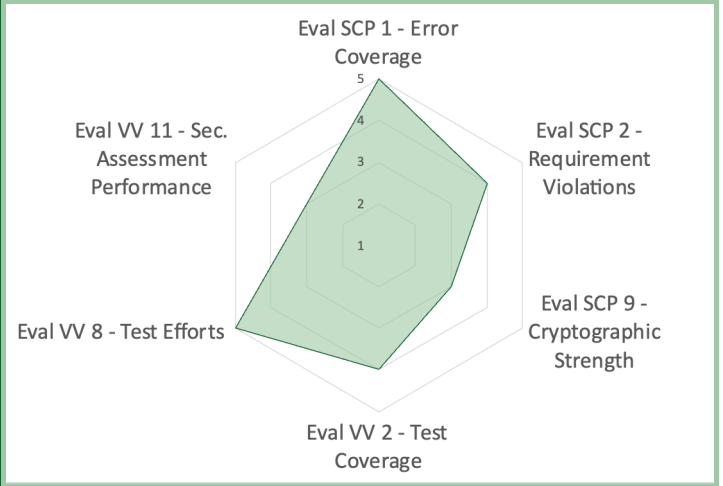




Connection between Demonstrator and V&V Methods and Tools



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

cardio id

CISTER Research Center in Real-Time & Embedded Computing Systems

UNIVERSIDADE D COIMBRA

isep Instituto Superior de Engenharia do Porto

P.PORTO

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

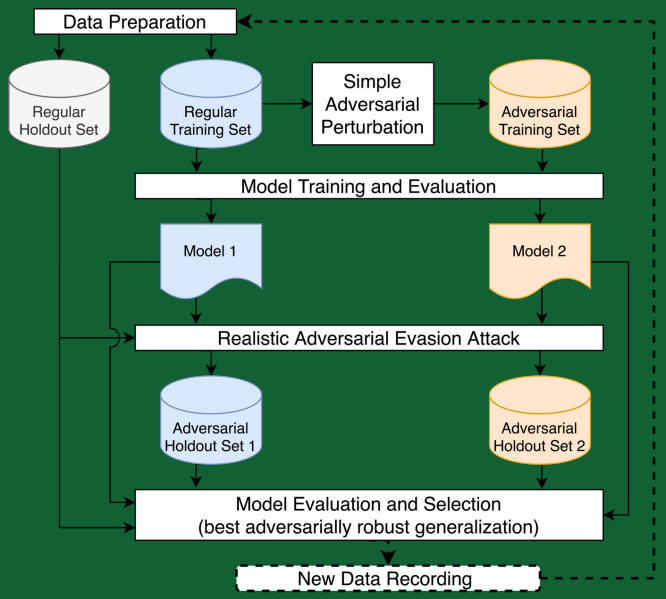
Contact person for the demo

Maytheewat Aramrattana
(maytheewat.aramrattana@vti.se)

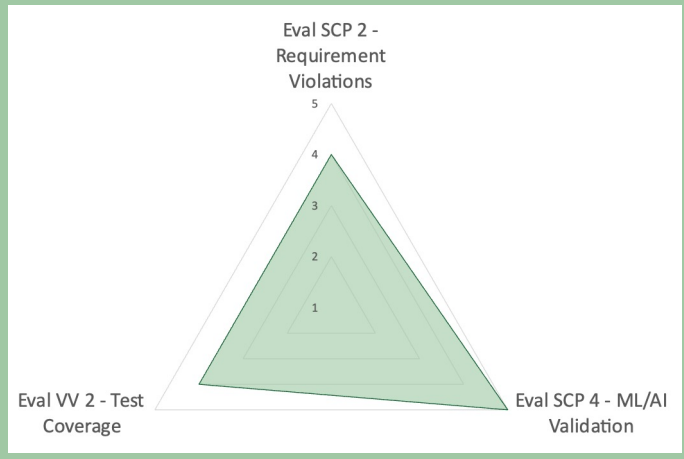
Impressions

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.

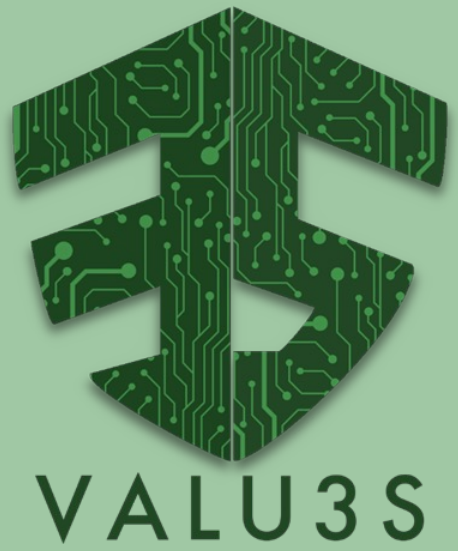
Participating partners

vti cardio4id gecad ISEP INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO

Thanks to all participants
for the great project!

VALU3S

ECSEL JU



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.