Overview of Robotics Testing Services

1 Introduction

This paper gives an overview of the testing services and the verification and validation research activities at T&VS and the University of Bristol at the Bristol Robotics Laboratory (BRL), respectively.

2 Basic Architecture of T&VS Tooling Solutions for Robotics Testing

The following diagrams describe architectures of robotics simulation test benches developed at the University of Bristol as part of the RoboSAFE research project.

2.1 Test bench architecture for testing robot high-level control state machine

Figure 1 "Test bench architecture for testing robot high-level control state machine" below shows an overview of the basic test bench architecture for verifying high-level robotics control software (as distinct from the low-level software controlling sensors and actuators, sometimes referred to as firmware).

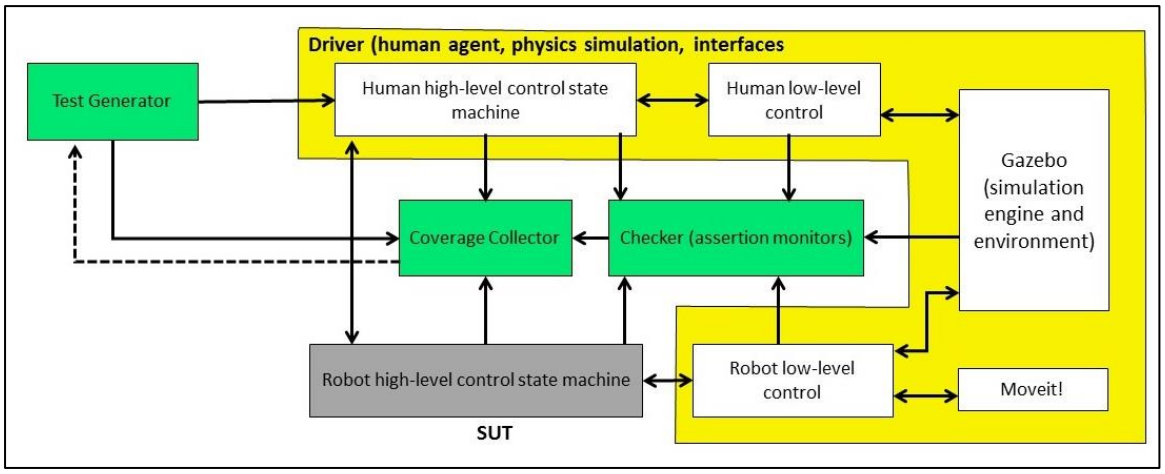

Figure 1: Test bench architecture for testing robot high-level control state machine used in RoboSAFE

Explanation of above diagram:

- **Test bench elements in green**: The test bench elements are shown in green. They generate stimulus, collect coverage and check responses. The coverage collectors are used to measure the quality of the testing, based on a variety of complementing coverage models including code-based, structural, functional, assertion and requirements coverage. The generator is "active" (i.e. driving stimulus) whilst the coverage collector and checker are passive (i.e. only monitoring activity).
- **Driver in yellow**: Running in ROS (Robot Operating System)
    - Human interaction is modeled through high level models (using state machines) and lower level drivers that implement the higher-level actions
    - Gazebo is the simulation environment

    - The robot low-level control is the driver firmware that implements the high-level actions coming from the high-level robot control state machine
    - Moveit! Is used to model robot movements
- **SUT:** Software Under Test
    - The SUT is the high-level robot control software encoded as a state machine for the purpose of the RoboSAFE research project

The code that implements different research prototypes for this testbench architecture is available on github under https://github.com/robosafe.

Using the above test bench architecture, it is possible to define tests using T&VS tools and libraries, drive the test stimulus through to the ROS environment and hence to the robot. The models in the ROS environment are able to interact with the robot code in simulation and hence provide a realistic test environment.

Figure 2 "Overview of test bench architecture for testing robot high-level control state machine as used in [1] and [2]" below gives a less detailed view of the test bench architecture. The architecture depicted in Figure 2 was developed as part of implementing a Coverage-Driven Verification (CDV) methodology in RoboSAFE. More details on CDV are given in "Coverage-Driven Verification - An Approach to Verify Code for Robots that Directly Interact with Humans" [1], where the basic test bench architecture and CDV methodology are introduced, and in "Systematic and Realistic Testing in Simulation of Control Code for Robots in Collaborative Human-Robot Interactions" [2], where the use of constrained random test generation is compared to model-based test generation techniques in the context of CDV.

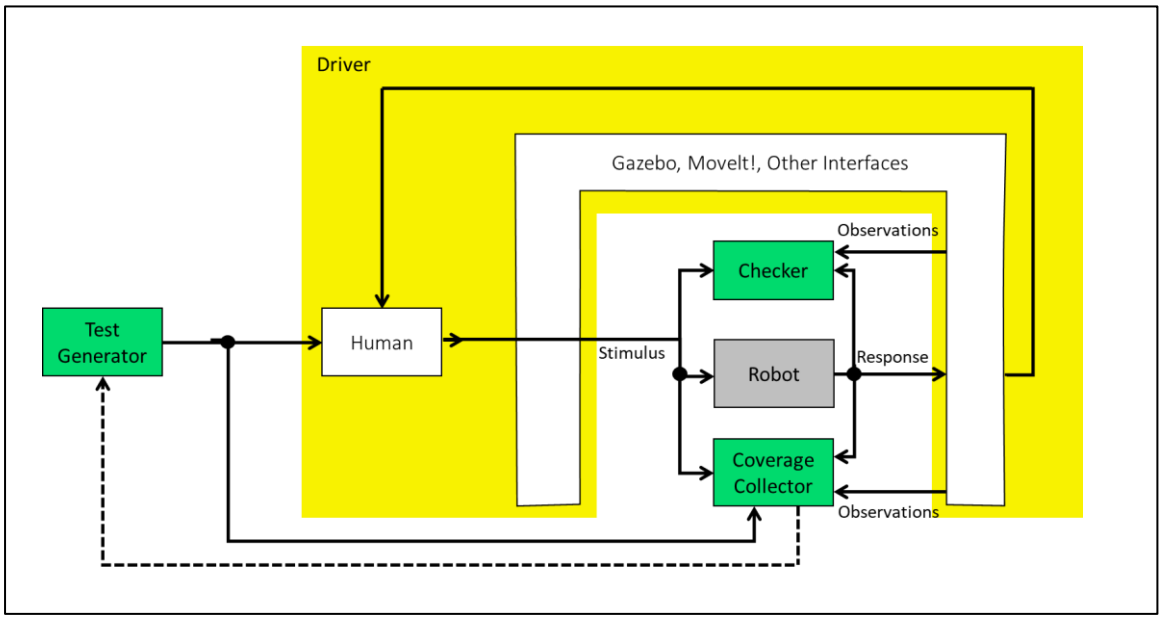

Figure 2: Overview of test bench architecture for testing robot high-level control state machine as used in [1] and [2]

3 T&VS tooling solution

The T&VS tools and libraries that can be used to implement the test benches depicted in Figure 1 "Test bench architecture for testing robot high-level control state machine" and Figure 2: Overview of test bench architecture for testing robot high-level control state machine as used in [1] and [2]" above can be developed as part of a SystemC test bench verification solution based on the Universal Verification Methodology (UVM). This tooling (named TVM) was made feely available for others and has been used in several software and robotics testing projects in collaboration with the University

of Bristol and other projects (see Section 2 “Basic Architecture of T&VS Tooling Solutions for Robotics Testing”, Section 4.1 ”V&V of Autonomous Systems”, Section 4.4 “Automotive V&V and Safety”).

4 T&VS Research Projects

4.1 V&V of Autonomous Systems

T&VS investigated the feasibility of applying Advanced Hardware Verification Techniques to the testing of software for Cyber Physical Systems. See the project page for more information.

4.1.1 Testing of Thales Autonomous Marine

Under this project T&VS worked very closely with the Thales testing team. The Thales team use the MOOS simulator to test their control software within a simulated environment. T&VS integrated their tooling to randomly (using constrained random scenarios) inject multiple marine vehicles with random movements. T&VS then checked the reaction of the Software Under Test using assertions and used metrics to measure how much testing had been performed (see Figure 3 “T&VS Tooling Integrated with MOOS” below).

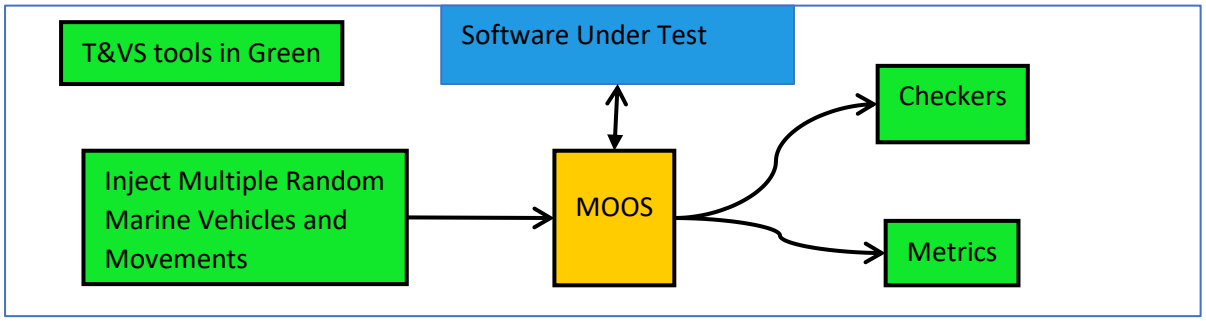

Figure 3: T&VS Tooling Integrated with MOOS

4.2 PEnDAR - Performance ENsurance by Design, Analysing Requirements: Integrating Performance V&V into Standard Processes

This project is aimed at explicitly considering performance requirement in the design process rather than as an emergent property from the design process. T&VS have investigated the following and incorporated their results into this report:

- The feasibility of integrating performance V&V into a safety standards-compliant process suitable for safety-critical applications such as automotive.
- Extending existing standards-compliant requirement sign-off tools to manage the capture and decomposition of performance/resource V&V requirements into specifications, features and sign-off criteria.
- How the performance V&V process can be incorporated into a standards-compliant workflow for safety-critical applications.

See the project page for more information.

4.3 National Aerospace Technology Exploitation Programme

T&VS developed a tool (asureSIGN™) to support Requirements Based Verification for DO-178 & DO-254 compliance in aerospace software and hardware development. Both standards mandate that developers demonstrate key safety requirements have been fully tested and that test coverage targets have been met.

asureSIGN™ is uniquely placed to interface to the already establish Requirement Management tools such as Doors and to automated testing tools to provide a completely automated tool-independent

solution to demonstrate standards compliance for testing. Combining both software testing and hardware verification tracking into a single platform thus allowing clients to more efficiently test their products which increasingly combine complex software and hardware solutions.

T&VS worked closely with a research team at the University of Bristol and end-user partner Rolls-Royce. Rolls-Royce provided domain expertise input through to feature prioritization and implementation review in each phase, and finally full evaluation of the tool on a candidate project.

See the project page for more information.

4.4 Automotive V&V and Safety

T&VS will be involved in two new research projects both involving the testing of autonomous vehicle software

4.4.1 Robopilot

Robopilot will develop & demonstrate autonomous driving functionality for Charge's new electric Light Commercial Vehicle (LCV). It brings advanced technology developed by Charge for the Roborace autonomous race series to the traditionally conservative LCV market and will be followed by heavier trucks and buses. Charge plan to gain market share by providing electric powertrains at the same payload and price points as traditional vehicles, achieved by a new and revolutionary chassis and body design and build process. Charge also plan the 'digitisation' of the vehicle to fully integrate vehicle, fleet and depot delivery management systems for more efficiency. The progressive roll-out of autonomy via OTA (Over The Air) updates is another disruptive market differentiator that will help gain market share and demand has been confirmed in discussion with major fleet customers such as UPS and through involvement in international activities organised, for example, by the OECD ITF or the US FMCSA. The project includes a full assessment of vehicle safety, evaluation and hardening of cyber-physical security, and an approach for verification and validation of the autonomous decision-making algorithms. Demonstration of SAE L4 autonomy will be over a 10-mile route on mixed public roads in all weathers, and of driverless parking/manoeuvring in customer depots.

This will include system validation and verification using a state of the art cost and time efficient methodology, originally developed at the University of Bristol and to be commericalised widely by Test and Verification Solutions (T&VS). Systems will undergo simulation, hardware in the loop simulation & in-vehicle testing. Physical testing using specialised soft target test equipment will test extreme operation cases and confirm simulation results. Test procedures & simulation activity will be defined by the safety case led by Loughborough University who have an international reputation as experts in accidentology. Cyber security is critical for safe deployment of connected and autonomous vehicles. In Robopilot, Thales will will assess potential threats; the vulnerabilities of the T4 'drive-by-wire' Light Commercial Vehicle (LCV), control systems and communication paths; and will apply appropriate mitigations and demonstrate them. Thales will apply this approach and these solutions to the wider market for all types of CAVs.

See the project page for more information.

4.4.2 CAPRI

The CAPRI project will design & deliver a complete, market ready, mobility service deployable in urban scenarios on public roads and working with traffic signals using trusted secure PODs and systems supported with legal, regulatory, insurance recommendations for operation. The project will culminate in a series of trial deployments which systematically work towards demonstration of increasingly complex POD-based mobility services. These mobility services will be co-designed with real users to meet their needs and expectations and create an excellent user experience. Project outputs form a 'complete package' of products & services, viable business cases, insurance and legal

solutions to enable locations to quickly and easily deploy POD mobility services. The project therefore addresses all of the CCAV priority areas, with a particular focus on innovative business models based around POD mobility services, cyber-security of data & vehicle systems, validated real-time control systems and data management, with safety-assured machine learning and artificial intelligence.

T&VS is leading the work package on safety & security including cyber-physical security, methods & tools for verification & validation, road simulation, and regulatory recommendations. There are also specialist tasks in 'accidentology' research, verification and validation, advanced test generation, and simulations. CAPRI's development of rigorous V&V methods and tools for testing complex autonomous systems departs from conventional verification of software components to measure decision-making correctness & safety in a highly complex environment, which may include experiential & shared learning; it will potentially provide a basis for future vehicle type approval and a digital MOT for all autonomous vehicles, not just PODs

See the project page for more information.

5 T&VS Industrial Safety Projects

See Safety Compliance page for additional information on the T&VS compliance solutions.

5.1 Medical

Creo Medical, a manufacturer of clinically innovative medical devices, called upon Test and Verification Solutions (T&VS) to establish a unit testing strategy for the software it was developing for its CROMA system, an electrosurgical unit that delivers bipolar radio frequency power for the purpose of cutting and microwave power for the purpose of coagulating tissue to staunch bleeding vessels.

T&VS was subsequently contracted to undertake unit testing of the software that was completed on schedule, enabling Creo Medical to proceed with certification of the CROMA system software to the medical device software safety standard, IEC 62304.

See the project page for more information.

5.2 Avionics

A global provider of high integrity electronic control systems to the aerospace industry selected T&VS to undertake a compliance review of the system requirements for an aircraft Steering Control Unit (SCU) which takes inputs from the pilot tiller and rudder control pedals and controls the nose wheel position and movement.

The purpose of the compliance review was to confirm that the system requirements:

- Comply with higher level (customer) requirements
- Are traceable to higher level requirements or are derived requirements resulting from the solution design
- Are consistent and accurate
- Are verifiable
- Have accurate algorithms
- Are compatible with the target computer
- Conform to standards

See the project page for more information.

5.3 Industrial IEC61508

T&VS undertook a review of development processes for a large UK company developing industrial products that needed to comply with IEC61508. The details on this are confidential.

5.4 Automotive ISO26262

T&VS performs a wide range of ISO26262 compliance activities including IP level and SoC ISO26262 compliant verification (some using asureSIGN). T&VS also performs fault injection simulations to ensure designs are able to identify faults and recovery from single fault issues.

5.5 Security

T&VS helps organisations to ensure their products are secure. This project page shares an example from the Oil and Gas industry.

6 University of Bristol Research Projects at BRL

6.1 RoboSAFE

See http://www.brl.ac.uk/research/researchthemes/verificationvalidation/robosafe.aspx

As the EPSRC's "Principles of Robotics" document states: "Robots are products - they should be designed using processes which assure their safety and security".

The RoboSAFE project brings together users of such robots with those researching the verification and validation of autonomous systems, to address these safety issues and so provide a holistic methodology for verification and validation that enables the design of safe and trustworthy robotic assistants.

As part of RoboSAFE, the University of Bristol demonstrated the benefits of using Coverage-Driven Verification to automate a large part of simulation-based testing of code used to control robots that directly interact with humans on the example of a human-robot collaborative manufacturing task, resulting in a novel test bench architecture for robotics verification in ROS. We then focused on the problem of efficiently generating effective tests. We developed a very effective model-based approach that made use of the models developed for formal verification and model checking in the test generation process. This approach is capable of directing test generation to hard to reach and critical interaction scenarios. To further increase the level of automation, we then introduced agency into the verification environment by modelling the human and the environment the robot interacts with as agents. Our most recent results show that using multi-agent systems as models for test generation is as effective as the more traditional method of model checking automata, with the extra benefits of multi-agent models being small, measured in the number of lines of code when compared to the automata, and model traversal time being low and constant.

6.2 RIVERAS

See http://www.brl.ac.uk/research/researchthemes/verificationvalidation/riveras.aspx

One of the greatest concerns about autonomous intelligent machines is whether they are safe and dependable. In the RIVERAS project we develop techniques that enable system designers to gain confidence in the correctness of the autonomous intelligent systems they create. To achieve solutions that make a difference in practice, we exploit novel combinations of established techniques sourced from state-of-the-art microelectronics design verification, control engineering, mathematical logic and automatic theorem proving. For example, to verify state-of-the-art control systems, designed in Simulink, we have proposed the use of both simulation as well as proof-based techniques [4,5]. Our techniques either provide a convincing evidence, including proof, that autonomous systems always perform as specified, or that the likelihood of failures meets system requirements.

RIVERAS places special importance on the design process, with a focus on specification and design space exploration. Traditionally, verification requires a specification that fully defines the functional behaviour of a system. However, such specification may not be available for systems that are expected to adapt to unforeseen circumstances; there are far too many possible scenarios for this to be practical. Instead, in RIVERAS we are developing flexible specifications expressed in terms of acceptable and required behaviour with associated precise limits for critical properties complemented by more vague indications of desired actions.

6.3 Research Papers

1. D. Araiza-Illan, D. Western, A. Pipe, and K. Eder, "Coverage-Driven Verification: An Approach to Verify Code for Robots that Directly Interact with Humans," in Haifa Verification Conference, Haifa, Israel, 2015. http://link.springer.com/chapter/10.1007/978-3-319-26287-1_5
2. D. Araiza-Illan, D. Western, A. G. Pipe, and K. Eder, "Systematic and Realistic Testing in Simulation of Control Code for Robots in Collaborative Human-Robot Interactions," in Towards Autonomous Robotic Systems (TAROS), Jun. 2016. http://link.springer.com/chapter/10.1007/978-3-319-40379-3_3
3. D. Araiza-Illan, A. G. Pipe, and K. Eder, "Intelligent Agent-Based Stimulation for Testing Robotic Software in Human-Robot Interactions," in Third Workshop on Model-Driven Robot Software Engineering (MORSE), Leipzig, Germany, 2016. https://doi.org/10.1145/3022099.3022101
4. D. Araiza Illan, K. Eder, A. Richards. "*Formal Verification of Control Systems' Properties with Theorem Proving,"* International Conference on Control (CONTROL), pp. 244 - 249. IEEE, Jul 2014. http://dx.doi.org/10.1109/CONTROL.2014.6915147
5. D. Araiza Illan, K. Eder, A. Richards. "*Verification of Control Systems Implemented in Simulink with Assertion Checks and Theorem Proving: A Case Study*," European Control Conference (ECC), pp. 2670 - 2675. Jul 2015. http://arxiv.org/abs/1505.05699