Testing Complex Cyber Physical Systems with a Safety Framework

Mike Bartley, TVS
Agenda

- About TVS
- What are cyber physical systems?
- What are the opportunities and challenges?
- Applying Hardware Verification Techniques in Software Testing?
  - Constrained random techniques
  - Functional Coverage
  - Assertion-based checking
- Compliance to Safety Standards
  - Requirements-Driven Test and Verification
About TVS

• Focused on HW verif and SW test
  – Services
  – Products
• 130 engineers worldwide
• Trusted by wide range of clients and partners
• Delivering T&V Solutions since 2008

Helping companies develop products that are: Reliable, Safe and Secure
What are cyber physical systems?

- Cyber-Physical Systems (CPS) are integrations of computation, networking, and physical processes.
- Embedded computers and networks monitor and control the physical processes, with feedback loops where physical processes affect computations and vice versa.
- They may also have some self-learning aspects but this is not a necessity.
Examples of Cyber Physical Systems

- Dyson Autonomous Vacuum Cleaner

  ![Dyson Autonomous Vacuum Cleaner](image)

- **Must**
  - Be good at cleaning the room
  - With minimal floor coverage
  - SAFELY!
Examples of Cyber Physical Systems

- **Autonomy and Offboard Systems**
  - Unmanned Surface Vehicle steers its way from A to B
  - Potentially towing a payload
  - Steering clear of obstacles and collaborating with Unmanned Underwater Vehicles
  - Communicating via a central operations centre
  - Multiple goal driven behaviours

- **Must**
  - Get from A to B
  - With minimal time and fuel
  - SAFELY!
Examples of Cyber Physical Systems

- Autonomous Vehicles

- Must
  - Get from A to B
  - With minimal time and fuel
  - SAFELY!
Opportunities and Challenges

- For example: Automotive
  - ADAS and Driverless cars
  - Electronics in automotive is set to rise at 19% per annum for the next 5 years

- Many other opportunities
  - Drones, IoT, robotics, etc.

- These new systems have many challenges
  - Safety
    - Demonstrating compliance to standards (e.g. ISO26262, DO254/178C)
  - System Complexity impacting V&V
The V&V Challenge

- Cyber Physical Systems introduce a complex software testing challenge
  - A large input space
  - Difficulty predicting expected response

- Hardware faced a similar problem 20 years ago
  - Over the past 20 years a number of “Advanced Hardware Verification Techniques” (AHVT) have been introduced
  - To automate test generation and response checking

- Can this be done within a safety framework?
The Innovate UK Research Project

- Investigate the feasibility of applying Advanced Hardware Verification Techniques to the testing of software for Cyber Physical Systems
  - Technical feasibility
  - Market feasibility

- TVS
  - Producing tools for evaluation by end user partners

Test generation from formal models
Robotic Vacuum Cleaner
Software for Autonomous Vehicles
Autonomy and Offboard Systems
Advanced Hardware Verification Techniques

Software Requirements

Test Plan

Test Results

Coverage

Checker

Monitor

Constrained Random Input

Formal Model

Software Under Test

Active
Passive

Doors, etc
Results of Bubble Sort “Proof of Concept”

Lists of
- Integers
- Floats
- Ascii
- etc

Constrain towards
- Empty lists
- Equal values
- Reverse ordering

List Generator

Checkers

Software Under Test

Coverage Metrics

- Empty List
- Reverse ordered
- Error cases (mix integers, floats, ascii
- etc

Lists of
- Integers
- Floats
- Ascii
- etc

• Check output list is ordered
• Output list contents == input list contents
Example Constrained Random Inputs

- **Mimic sensor input data**
- **Need to constrain those inputs**
  - Only the legal space
  - Hit the corner cases

- **Example scenarios**
  - Valid ranges for data
  - Relationships between inputs
  - Next input within certain “distance” to prior input
Functional Coverage

From Kerstin Eder of the University of Bristol

- Requirements coverage
- “Cross-product” coverage


A cross-product coverage model is composed of the following parts:
1. A semantic **description** of the model (story)
2. A list of the **attributes** mentioned in the story
3. A set of all the **possible values** for each attribute (the attribute value **domains**)
4. A list of **restrictions** on the legal combinations in the cross-product of attribute values

A **functional coverage space** is defined as the Cartesian product over the attribute value domains.

- Situation coverage

Example Checkers

- **Do not accelerate too fast**
  - Assert that output to motor is not too high

- **“always respond correctly”**
  - If A&B&C occur then check X happens
    - Assertion coverage “check A&B&C occurs” for free

- **Always safe**
  - Do not get too close to other objects
  - Requires some level of modelling

- **Minimise resources**
Safety compliance (asureSIGN)

- Managing Requirements
  - Importing and editing requirements

- Decomposing requirements to verification goals

- Tracking verification execution
  - Automating import of verification results (VectorCAST)
  - Automate accumulation and aggregation of verification results

- Impact analysis
  - Managing changes in requirements and verification

- Demonstrating safety compliance – for example
  - DO254/178C, ISO26262, IEC 60601, IEC 61508, EN 50128, IEC 61513

- Supply chain management
  - Exporting requirements and test plans
  - Importing test results
asureSIGN™ at the heart of HW/SW V&V

Requirements
- Excel
- Doors
- Jira
- Etc
Word via XML

SystemC Simulation

Hardware Simulation
- Coverage Cadence
- Assertions Mentor, Aldec
- Etc.

Formal Verification
- OneSpin

Directed test results

Automated SW Test Tool
VectorCAST

Lab Results

Manual API

Run API

Matlab

SW Test Tools

Requirements Engineering tools
The Status and the Opportunity

http://www.testandverification.com/projects/

- **Requirements Driven Verification**
  - Tool released to partners

- **Partner V&V Requirements Analysis**
  - Understanding how to adapt AHVT to software
  - Tooling being adapted
    - Checkers
    - Coverage
    - Test Generation

- **The Opportunity**
  - Able to deliver the tooling to new partners
  - Contact Mike Bartley
    - mike@testandverification.com 07796 307958
Conclusions

- The market opportunity is there
- But there are barriers to entry!
  - Demonstrating compliance to safety standards
  - System Complexity impacting Software V&V

TVS Solutions
- Requirements Driven Test and Verification – PROVEN
  - Automated with VectorCAST
  - asureSIGN – PROVEN
  - Constraint-driven testing with functional coverage & assertions
    - Hardware – PROVEN
    - Software – partially PROVEN, working with partners

Get Involved
Contact details

- Mike Bartley
- mike@testandverification.com
- 07796 307958