A TOOL-CHAIN FOR FUNCTIONAL SAFETY AND RELIABILITY IMPROVEMENT IN AUTOMOTIVE SYSTEMS


reda.nouacer@cea.fr
smail.niar@univ-valenciennes.fr

https://equitas-project.com/site/

Bpifrance AAP FUI16 and the General Council of Essonne France
AGENDA

- Context and Trends
- Objectives and Results
- Methodology and tools
  - Technical challenges
  - Automatic test generation
  - Analysis and verification of compliance with the requirements
  - Virtual platforms and HW faults injection
- Current status – Tools chain V2
- Next works
CONTEXT AND TRENDS

- **μElectronic Miniaturization**
  - Increased sensitivity of ECU to transient hardware faults
- **Increased number of functions**
  - 10-100 ECU (distributed system)
- **Hostile operating environment**
  - Electromagnetic fields, temperature, humidity
- **ISO26262 standard**
  - Safety constraints (product and process)
- **Embedded software V&V**
  - Complex iterative process
  - 40-50% total development cost
BLOC DIAGRAM OF CONTROL LOOP

Instructions
(e.g. windshield wiper " commodo")

Analysis and decision

monitoring and control system
(e.g. BCM)

Measurements / Interruptions

Inputs
(e.g. CAN, ADC)

Sensors

Driven process
(e.g. Wiper blades)

Outputs
(e.g. CAN, PWM)

Actuators

Disturbances
(e.g. Dirt, wind, age, T°C, magnetic field)

Physical system
(e.g. USM)

Inputs
Outputs

ENHANCED QUALITY USING INTENSIVE TEST AND ANALYSIS ON SIMULATORS
FUNCTIONAL SAFETY AND RELIABILITY ANALYSIS

- Test Bench
- Embedded System
- Data Analyzer
- Fault Scenarios
- Tolerance Scenarios
- Injection
- Reference
- Reliability Model
OBJECTIVES AND RESULTS

- Automate the verification and validation process of whole embedded software stacks
  - By developing a continuous tool-chain
  - In the context of automotive electronic systems

- Improve the relevance of the test campaigns
  - By detecting the redundant tests using equivalence classes

- Provide assistance to the hardware failure effect analysis (FMEA)
  - By introducing a hardware faults model during simulation.

- Extract a comprehensive V&V methodology using virtual platforms
  - By assessing the EQUITAS tool chain on real automotive use cases

- Assess the tool-chain under the ISO 26262 requirements.
ENHANCED QUALITY USING INTENSIVE TEST AND ANALYSIS ON SIMULATORS

VIRTUAL TESTING ENVIRONMENT

Exigences

Modèle de test

Modèle comportemental

MaTeLo & DIVERSITY

Scénarios de test

[ Driver = Adapter + Controller ]

UNISIM-VP & Fautes Matérielles

CAN, ADC,

CAN, PWM,

Environnement physique

ARTiMon (Checkers)

Traces d'exécution

Verdicts

Environnement de test

Observer

Observer

Observer

Observer

Moteur d'exécution des scénarios

Séquenceur

Driver

Driver

Driver

Driver
ENHANCED QUALITY USING INTENSIVE TEST AND ANALYSIS ON SIMULATORS

METHODOLOGY & TOOLS

- Tool-chain Inputs
  - Environment Model
  - Source Code
  - System Model
  - System Requirements

- Test Plan Elaboration
  - Code Generation
  - Test Cases Generation
  - Test Cases
  - Requirements Translation

- Compilation
  - Embedded Code
  - Compilation
  - Executable Binary

- Virtual Execution
  - Environment Simulation
  - Embedded Target Simulation

- UNISIM-VP & PhiSim

- Analysis
  - Execution Traces
  - Requirements Verifications & Analysis

- Verdict
  - Alerts
  - ARTiMon

DIVERSITY & MaTeLo

METHODOLOGY & TOOLS

- Virtual Execution
  - Environment Simulation
  - Embedded Target Simulation

- Compilation
  - Embedded Code
  - Compilation
  - Executable Binary

- Test Plan Elaboration
  - Code Generation
  - Test Cases Generation
  - Test Cases
  - Requirements Translation

- Tool-chain Inputs
  - Environment Model
  - Source Code
  - System Model
  - System Requirements

- Analysis
  - Execution Traces
  - Requirements Verifications & Analysis

- Verdict
  - Alerts
  - ARTiMon
TECHNICAL CHALLENGES

- The use of symbolic execution principle to analyze and reduce test cases obtained by a stochastic approach
  - MaTeLo: stochastic test generation technique
    - Generate the most likely tests
    - Many redundant/duplicate tests
    - Developed by ALL4TEC (http://www.all4tec.net/MaTeLo/homematelo.html)
  - DIVERSITY: symbolic execution
    - Model validation by analyzing its symbolic execution tree
    - Property verification
    - Automatic test generation based mainly on the paths coverage
    - Developed by CEA LIST (http://projects.eclipse.org/proposals/diversity)

- The extension of the simulation environment UNISIM-VP
  - Modeling and injection of characterised hardware faults
  - Interface to test cases generation tools (MaTeLo & DIVERSITY)
  - Interface to compliance (monitoring) analysis tool (ARTiMon)
FUNCTIONAL SAFETY AND RELIABILITY ANALYSIS

Test Bench → Embedded System → Data Analyzer

Fault Scenarios

Reference

Injection

Reliability Model

Tolerance Scenarios
AUTOMATIC TEST GENERATION

MATELO OVERVIEW

1 Graphical Design
2 Test Case Generation
3 Test Script Generation
4 Coverage Report

http://www.all4tec.net/MaTeLo/homematelo.html
COUPLING DIVERSITY AND MATELO

- **Test model**
  - Test model editor (MaTeLo)
  - Test model « MaTeLo format »
  - Stochastic test generation (MaTeLo)

- **Use case**
  - Application model (Simulink)
  - Test model editor (MaTeLo)
  - Use case model xLIA
  - MaTeLo tests analysis using symbolic execution (Diversity)
  - Reduced MaTeLo test campaign
  - MaTeLo test campaign
  - Generation of the test campaign scripts for driving simulation

---

**Remove duplicates (40%)**

- Preserving software reliability
- Enhancing test coverage

**Reduction of overall test length**

- Reducing duration of test execution
- Reducing cost
- Preserving same test coverage
FUNCTIONAL SAFETY AND RELIABILITY ANALYSIS

Test Bench → Embedded System → Data Analyzer → Fault Scenarios → Reference → Reliability Model

Injection → Fault Scenarios

Tolerance Scenarios
ARTIMON: ADVANCED REAL TIME INFORMATION MONITORING

- Provides a temporized logic based language
  - To express requirements about system real-time behavior

- Transforms a set of requirements into operational detectors
  - For the simulation/execution environment

**ARTiMon 4 Simulink:**

![Diagram](attachment:image.png)

An invariant (a property that should be valid at any time):

\[
\text{when } (\text{Switch\_On and (it is always the case that Redzone holds on time range } [-3,0])) \text{ then (there exists at least one occurrence of Alarm on time range } [0,1.5])
\]
FUNCTIONAL SAFETY AND RELIABILITY ANALYSIS

Test Bench \rightarrow Embedded System \rightarrow Data Analyzer \rightarrow Fault Scenarios \rightarrow Injection \rightarrow Reference \rightarrow Reliability Model

Tolerance Scenarios
UNISIM – VIRTUAL PLATFORM

COMPONENT-BASED VIRTUALIZATION ENVIRONMENT

UNISIM-VP
Embedded target simulation

Third Party Tools

Virtual Platform

Services

- Co-simulation
- Test-bench database
- Existing tool-chains

- System on Chip
- Boards
- SystemC/TLM

- Debugger
- Test
- Monitor
- Trace analysis
- Profiling
- HW fault injection

https://unisim-vp.org/site/index.html
UNISIM – VIRTUAL PLATFORM

STAR12X – AUTOMOTIVE APPLICATION

UNISIM-VP
S12XEP100
Board
Simulator

RAM
FLASH
EEPROM

XGATE
CPU12X
MMC

ECT
XINT
PIT
CRG

ATDx
SCI
PWM
SPI
CANx

Debugger

ELF
Loader

S-Rec.
Loader

.s19
S-Rec.
binary

ABS ELF
binary

AUTOSAR
BSW+RTE

Third Party Tools Stubs

S12XEP100 Board

UNISIM – VIRTUAL PLATFORM

STAR12X – AUTOMOTIVE APPLICATION

UNISIM-VP
S12XEP100
Board
Simulator

RAM
FLASH
EEPROM

XGATE
CPU12X
MMC

ECT
XINT
PIT
CRG

ATDx
SCI
PWM
SPI
CANx

Debugger

ELF
Loader

S-Rec.
Loader

.s19
S-Rec.
binary

ABS ELF
binary

AUTOSAR
BSW+RTE

Third Party Tools Stubs

S12XEP100 Board

UNISIM – VIRTUAL PLATFORM

STAR12X – AUTOMOTIVE APPLICATION

UNISIM-VP
S12XEP100
Board
Simulator

RAM
FLASH
EEPROM

XGATE
CPU12X
MMC

ECT
XINT
PIT
CRG

ATDx
SCI
PWM
SPI
CANx

Debugger

ELF
Loader

S-Rec.
Loader

.s19
S-Rec.
binary

ABS ELF
binary

AUTOSAR
BSW+RTE

Third Party Tools Stubs

S12XEP100 Board
TEST CASE ENHANCED WITH HARDWARE FAULT INJECTION

Requirements file → Hardware target → Application

Fault quantifier → Fault probability of occurrence $P$

Fault injection engine & simulation (UNISIM-VP)

Test scenarios (MaTeLo)

Execution trace (code/data) with faults → Comparator and analyzer of execution traces

Reference execution trace (code/data)

Alert?

Yes → Reliability quantifier?
- Fault effects analysis
- Corrective Decisions
- Compute error ratio (MTTF)

No silence
FAULT INJECTION STRATEGY

1. Parameters list
2. Fault injection configuration
   - No
   - Fault injection activated
     - compute-probability()
     - P
     - inject-fault()
     - Generated fault injection trace

Test step
TOOLS CHAIN

Use case

Application model (Simulink)

System properties and requirements (test objectives)

Translation as monitoring specification (ARTiMon)

Test model

Test model editor (MaTeLo)

Translation to xLIA (Diversity)

Use case model xLIA

Stochastic test generation (MaTeLo)

Test model « MaTeLo format »

MaTeLo tests analysis using symbolic execution (Diversity)

MaTeLo test campaign

Use case model

Binary Code

Simulation

Embedded system +Simulink (Sys) +UNISIM-VP +HW Faults

Physical system +PhiSim

Test campaign in the standardized interpretable format

Generation of the test campaign scripts for driving UNISIM-VP & Simulink (MaTeLo)

ARTiMon

Compliancy analysis (ARTiMon)

Execution trace

Compliancy analysis (ARTiMon)

Verdicts

ARTiMon specifications

Execution trace

ARTiMon specifications

Translation to xLIA (Diversity)

Use case model

MaTeLo tests analysis using symbolic execution (Diversity)

MaTeLo test campaign

Stochastic test generation (MaTeLo)

Test model « MaTeLo format »

Test model editor (MaTeLo)

Test model

Use case

Application model (Simulink)
USE CASE

WINDSHIELD WIPER
NEXT WORKS

- Studying the compliancy of the EQUITAS toolchain with the ISO26262 standard.

- Quantitative and qualitative assessment of the toolchain, by the project industrial partners.

- Generalization of project activities
  - Distributed embedded systems
  - Heterogeneous (model, ASW, binary) validation and verification

- Extension of EQUITAS toolchain
  - RAMS analysis (Reliability, Availability, Maintainability, Safety)
A TOOL-CHAIN FOR FUNCTIONAL SAFETY AND RELIABILITY IMPROVEMENT IN AUTOMOTIVE SYSTEMS


reda.nouacer@cea.fr

https://equitas-project.com/site/

Bpifrance AAP FUI16 and the General Council of Essonne France