RTS NOTES

Paper clippings

September 7, 2016

Contents

1 On the effective use of Fault injection for the assessment of AUTOSAR safety mechanism

1.1 Key Idea

AUTOSAR safety standard ISO26262 strongly recommends usage of the fault injection standards, but no definite mechanism exists for enforcing the same. Representation of the faults using the standard fault models e.g. bit flips and data type based corruption are not sufficient to model real time behavior. The existing Fault Injection framework GRINDER is extended to support AUTOSAR and an assessment is provided.

1.2 Width and scope

Provide open source and ready to use framework to do Fault Injection. Dependability assessment on existing AUTOSAR timing monitor safety mechanism for identifying deficiencies and guidelines for derivation of special fault models, injection mechanisms and locations based on abstract AUTOSAR and ISO26262 fault models. Eariler approach mentioned include: Lanigan et.al. and Baugarten et al. First approach being based on VECTOR CaNoe and second approach used anotated SWC Component to introduce fault ports. Another approach is pre implementation testing using UML or AADL, in this failure level are assumed and the effect on model analysed. Vedder et. al extended property based testing to AUTOSAR. Here automated test cases were generated from a pre specified property files.

Hardware based FI: Modeling hardware error such as CAN bus failure, or NVRAM failure through corrupted CRC. Hardware based FI fails to handle component interaction and dependability property. Software based FI: e.g. BeSafe framework to intercept SWC calls and fuzzing error models to check resilience of SWC. GOOFI-2 to evaluate bit flip cases and MODIFI to check model at Simulink level.

Note: Simultaneous fault models with multiple points of failure completely missing from AUTOSAR standards.

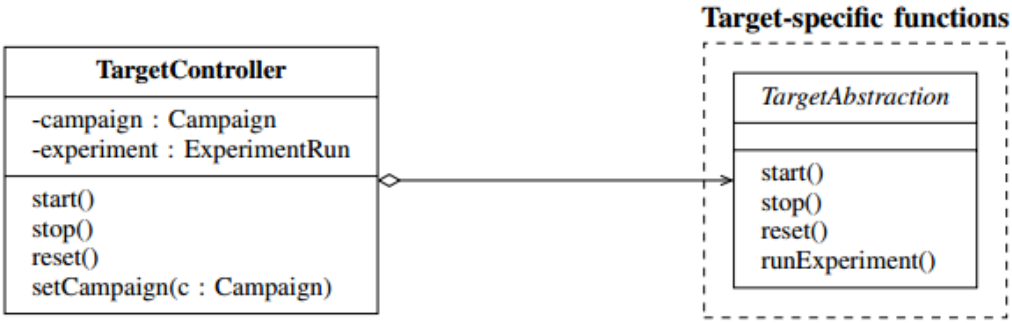

Figure 1: Abstract Target representation of GRINDER

1.3 Experimental approach

Configuration: Target is instrumented with injectors and detectors,. **Execution:** The target system is executed till the injection of fault and the perturbation data is successfully completed. **Evaluation:** The logs and traces are collected. GRINDER extended to AUTOSAR by providing a target specific implementation of TargetAbstraction Class with which GRINDER interacts during FI.

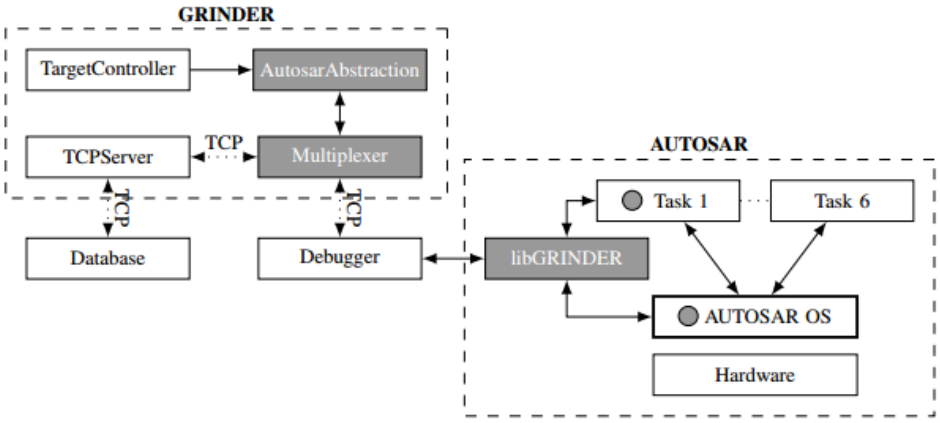

Figure 2: GRINDER new arch.

A case study is further done on Adaptive Cruise Control module.

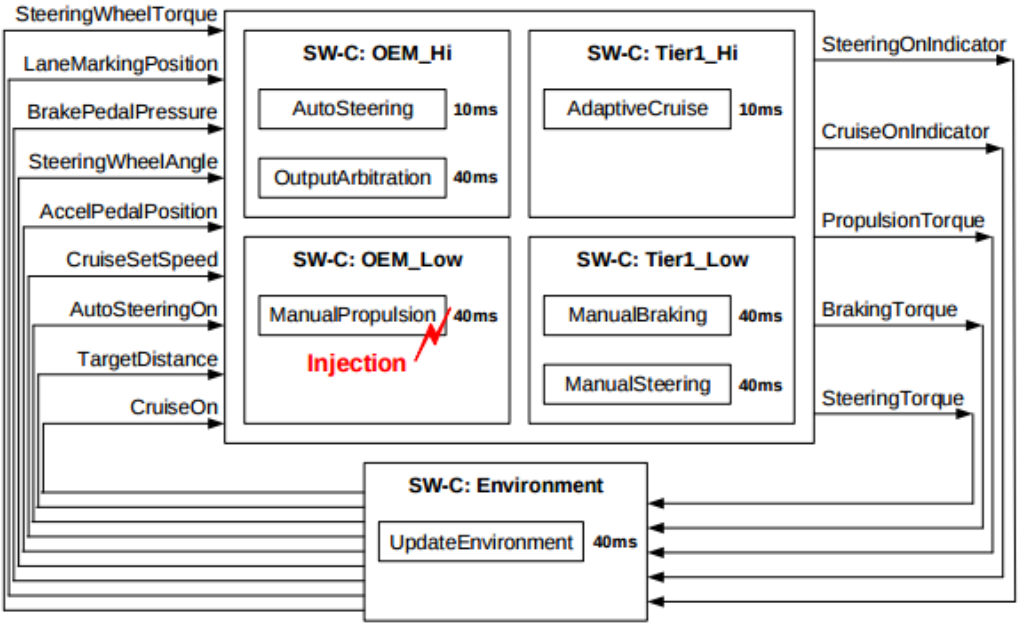

Figure 3: ABS Module architecture

Four different scenarios tested:

- Task timing error: Assess the correctness of the error detection and error mitigation of execution time monitoring. Analyze the propagation of the error with and without the presence of the timing errors.
- Interaction between the execution time monitoring and resource lock timing monitoring. Assess correctness and robustness of the mechanisms.

The task selection for monitoring ABS is shown below:

Task name	Priority	Runnable(s)
OEM_Hi_10ms	100	AutoSteering
Tier1_Hi_10ms	90	AdaptiveCruise
OEM_Hi_40ms	80	OutputArbitration
Environment_40ms	70	UpdateEnvironment
OEM_Low_40ms	60	ManualPropulsion
Tier1_Low_40ms	50	ManualBraking, ManualSteering

Figure 4: ACC task setup

1.4 conclusion

Detailed description of scenarios, A good framework to test the mechanism of fault injection and different failure scenarios. Can be used with possible change to JTAG interface to FTDI interface. Can be implemented as part of the eclipse plugin as as schedulability and testing mechanism.

1.5 Links

http://www1.deeds.informatik.tu-darmstadt.de/External/PublicationData/1/edcc-2015.pdf

References