U.S. DEPARTMENT OF ENERGY | Nuclear Energy

Office Of Nuclear Energy Sensors and Instrumentation Annual Review Meeting

Development and Demonstration of a Model Based Assessment Process for Qualification of Embedded Digital Devices in Nuclear Power Applications

Carol Smidts
The Ohio State University

NEET Project No.: 15-8097

October 18-19, 2017

Project Overview

Project Goal

- Develop an effective approach to resolve concerns about common-cause failure (CCF) vulnerabilities in embedded digital devices (EDDs)

Focus

- Address the challenge of establishing high levels of safety and reliability assurance for EDDs that are subject to software design faults, complex failure modes, and CCF

Project Overview (cont)

Objectives

- Assess the regulatory context for treatment of CCF vulnerability in EDDs
- Define a classification scheme for EDDs to characterize their functional impact and facilitate a graded approach to their qualification
- Develop and extend model-based testing methods to enable effective demonstration of whether devices are subject to CCF
- Establish a cost-effective testing framework that incorporates automation and test scenario prioritization
- Demonstrate the qualification approach through selection and testing of candidate digital device(s)

Project Participants

Participants

- The University of Tennessee (Richard Wood, Tanner Jacobi, Dan Floyd)
  - Assessment of regulatory requirements, classification of embedded digital devices, development of qualification approach.
- The Ohio State University (Boyuan Li, Carol Smidts)
  - Development of a generalized model-based mutation approach, prioritization of test cases, and automation of testing.
- Virginia Commonwealth University (Carl Elks, Tim Bakker Frederick Derenthal)
  - Development of model formalisms that can be used to derive effective test cases and application of fault injection techniques to extend test capabilities
- Analysis and Measurement Services Corporation (Brent Shumaker, Hashem Hashemian, Alex Hashemian)
  - Experimental assessment of the developed approach.

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Milestones Completed

- **M2CA-15-TN-UTK_-0703-034**
  - Develop classification approach for embedded digital devices (April 30, 2017)
- **M3CA-15-TN-UTK_-0703-035**
  - Select representative embedded digital device for testing and demonstration (June 30, 2017)
- **M2CA-15-TN-UTK_-0703-036**
  - Develop extended model-based testing methodology with integration and automation principles (September 15, 2017)
- **M2CA-15-TN-UTK_-0703-037**
  - Second Annual Progress Report on Development and Demonstration of a Model Based Assessment Process for Qualification of Embedded Digital Devices in Nuclear Power Applications (September 30, 2017)

Accomplishments
Embedded Digital Devices Classification

- **Embedded Digital Devices Classification**
  - Developed a classification framework for equipment with an EDD based on the functional roles allocated to the digital devices and the impact of their failure on the primary function of the equipment/instrument
  - Devised an analysis approach that extends the customary D3 analysis to account for the significance and functional impact of potential failures of an EDD and to enable a graded analysis approach based on classification of EDDs

Accomplishments Development of model-based testing framework

- Developed an automation method for the extended mutation testing framework in the requirements and design phase
  - Devising an automation strategy for mutant generation
  - Devising an automation method for mutant execution
  - Devising an automation method for mutant identification
  - Devising an automation method for test cases generation
  - Devising a prioritization method for mutant selection

Mutation Testing Introduction

- Mutation testing generates an effective test set.
- Mutation testing manipulates source code to generate mutants.
- An adequate test suite is able to distinguish all mutants

P

```
int Function1 (int in1, int in2) {
    int a, b, c, d, output;
    a = in1 + 3;
    b = in2 * 5;
    c = a ^ b;
…
```

M

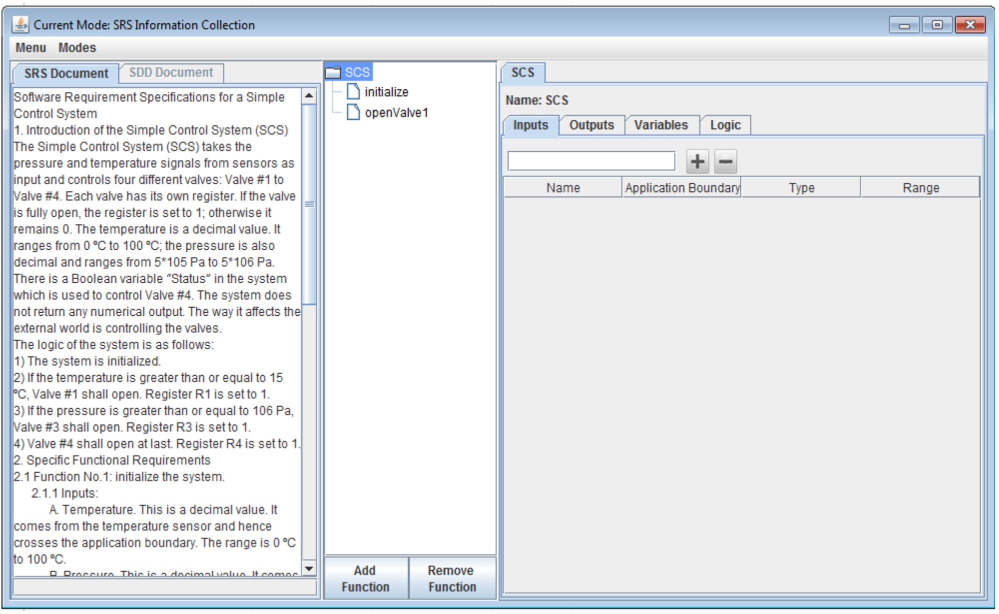
```
int Function1 (int in1, int in2) {
    int a, b, c, d, output;
    a = in1 + 3;
    b = in2 + 5;   // Mutated
    c = a ^ b;
…
```

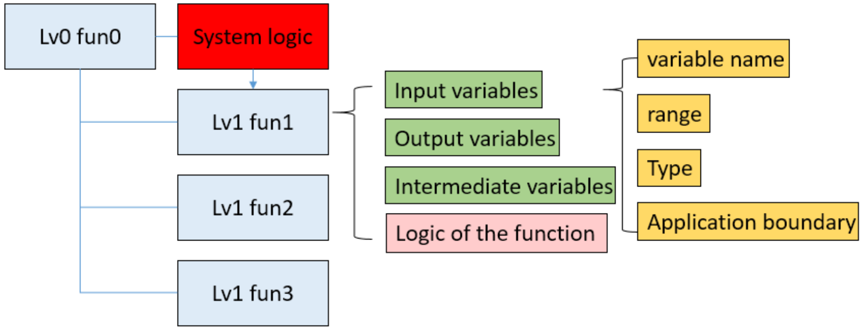
Development of model-based testing framework

- **Extension of traditional mutation testing to Requirements and Design level**
  - Traditional mutation testing focuses on the software code level and does not address requirements and design faults
  - To cover the full spectrum of possible faults, it is necessary to extend the mutation framework from coding faults to requirements and design faults.
    - Identification and classification of defects introduced in the requirements and design phase
    - Development of mutation operators for each defect category
    - Quantification of the number of mutants for each mutation operator
    - Preliminary development of a cost reduction strategy for each mutation operator
  - A large quantity of mutants is generated for testing. To implement the model testing framework, an automation method and tool is required

Automation of mutant generation

- **An automation strategy has been developed for mutant generation.**
  - The Automated Reliability Prediction System (ARPS) is a model-based software reliability assessment tool for safety critical software
  - ARPS models the Software requirements specification (SRS) and Software design description (SDD) using High level Extended finite-state machine(HLEFSM).
  - Mutants can be generated by revising the HLEFSM

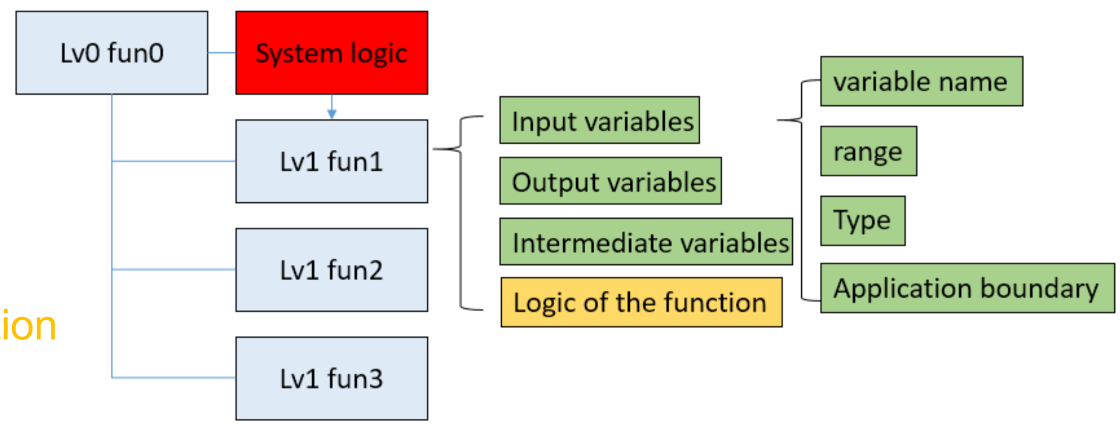




SRS/SDD Execution

Strategy of SRS/SDD execution

- Another key aspect is to be able to execute the HLEFSM of the SRS/SDD to identify defects. This is done in a phased approach:
  - Examination of functions definition
  - Examination of variables definition
  - Execution of each path the system traverses
  - Execution of each path a function traverses



- The execution results are outputted in a string by compiling the HLEFSM constructed by ARPS
  - E.g. in step 1, the execution result is shown as below. The level 0 function is placed in the square brackets. The higher-level functions are placed in the angle brackets.

[lv0 Fun0]<lv1 Fun1>< lv1 Fun2>< lv1 Fun3><…>

U.S. DEPARTMENT OF ENERGY

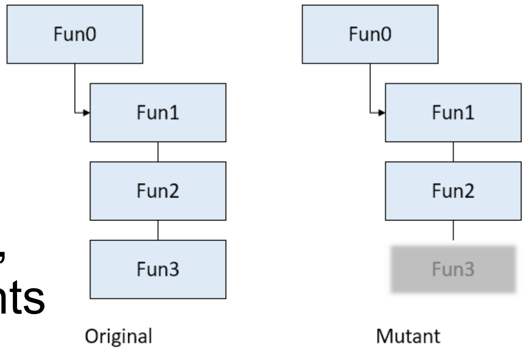
Nuclear Energy

Mutant Identification and test cases generation.

- **Mutants can be identified by comparing the results produced by executing the mutants.**
  - E.g. A Missing (definition of) Function mutant can be distinguished from the original application using the strings created.

    Expected output: [Fun0]<Fun1>< Fun2><Fun3>

    Mutant output: [Fun0]<Fun1>< Fun2>

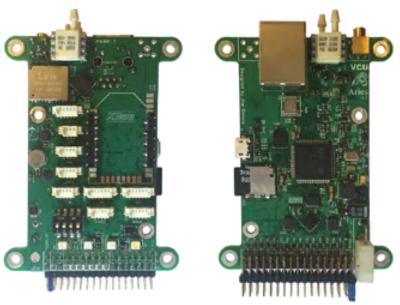


- **Test cases generation**
  - For mutants not identified by the existing test set, new test cases will be generated to kill the mutants using a Satisfiability Modulo Theories solver.

- **Prioritization methods were developed to further increase the cost effectiveness of the technique.**
  - These are based on EDD risk importance, function within EDD importance, fault class likelihood, mutant operator selection techniques

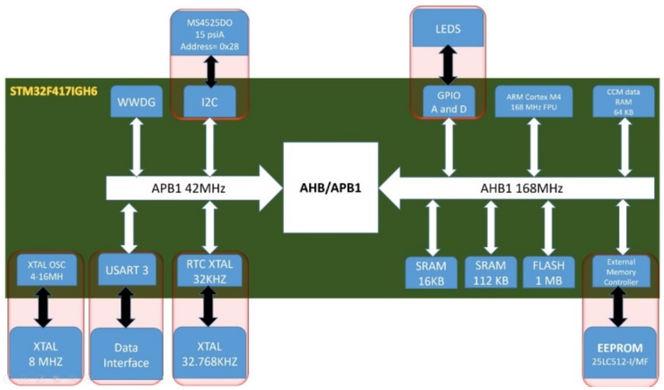
Accomplishments
Perform Experimental Testing and Evaluation

- **Two Versions: Hardware vs. Virtual hardware/software derived from the real VCU Smart Sensor**
  - Barometric pressure and temperature measurement device
  - Derived from a Part-23 (non-safety-related) VCU ARIES_2 Advanced Autonomous Autopilot Platform
  - Software
    - Real-Time Operating System – ChibiOS
      - Deterministic real-time multi-threaded scheduling
    - Drivers
    - Communication Layers



- **Purpose**
  - Demonstrate the efficacy of the methodology on an actual commercial EDD used in nuclear industry
  - Proprietary concerns over IP → VCU Smart Sensor
    - Representation of a commercial EDD
    - Guided by industry discussion (Schneider Electric, Foxboro) to ensure architectural features were representative of actual commercial devices

Smart Sensor



Features

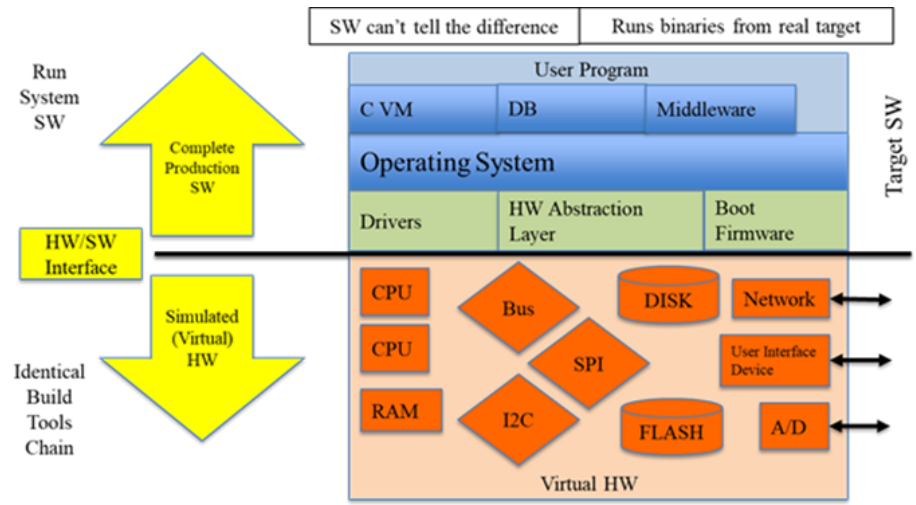
Temperature and pressure measurement
Altitude and airspeed measurement
Communication interfaces: I^2C, UART

Architecture

ARM STM32FM407 System on a Chip (SoC) device
Sensor head – MS4525DO

Functions:

Collection, display, and communication of measured data
Device configuration, storage of calibration information, performance of sensor functions



Virtual Platform

- Model of a hardware system that can run the same software as the hardware it models
  - Exact same architecture as the real hardware – accurately models the aspects of the real system that are relevant for software
- Allow for plant models to be integrated with the hardware/software model, placing the testing into plant context

Accomplishments

- **Presented project findings at the 2017 ANS Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC&HMIT) Conference in San Francisco, California**
  - Derenthal et al., “Virtualized Hardware environments for Supporting Digital I&C Verification”
  - T. Jacobi, et al., “Investigation of Instrumentation Containing an Embedded Digital Device”
  - B. Li and C. Smidts, “Extension of Mutation Testing for the Requirements and Design Faults”
  - R. Wood, H. Hashemian, B. Shumaker, C. Smidts, and C. Elks, “Development of a Model Based Assessment Process for Qualification of Embedded Digital Devices in NPP Applications: Research Approach and Current Status”

Technology Impact

- **Development of the Model-Based Testing Method:**
  - Provide effective demonstration of whether devices are subject to CCF
  - Establish a cost-effective automated testing framework for industry stakeholders to qualify equipment with EDDs

- **Resolution of Concerns Regarding CCF Vulnerability:**
  - Provide information to industry stakeholders on EDDs and CCF vulnerability
  - Reduce licensing, scheduling, and financial risk for utilities and reactor designers associated with utilizing digital equipment
  - Enable deployment of advanced instrumentation (e.g., sensors, actuators, microcontrollers, etc.) with EDDs
  - Lessen industry reliance on obsolescent analog technologies
  - Allow realization of the benefits of digital technologies

Activities for Third Year

- **Development of the model-based testing framework**
  - Implement the automation tool for the extended mutation testing in the requirements and design phase
  - Finalize the Virtual Platform simulation and the testbed automation framework
  - Assemble the physical smart sensor for baseline testing and establish the testing protocol
  - Generate and execute source code, requirements/specifications, and design mutants for the representative instrument
- **Perform Experimental Testing and Evaluation**
  - Further enhance the VCU smart sensor, as needed, with additional functionalities appropriate to the nuclear context
  - Integrate the test subject and testbed to execute test cases and verify the sufficiency of the test set using scripting methods
  - Perform baseline and MBT experimental testing
  - Evaluate testing results and perform comparative analysis to confirm the capabilities of MBT

Conclusion

- **The practical methods, tools, empirical data, and demonstrations that results from this research effort will:**
  - Facilitate digital I&C qualification activities for advanced instrumentation technology for deployment in the industry
  - Support reactor vendors and utilities in assessing I&C design and modernization options without substantial regulatory risk and implementation costs

- **This research establishes advanced sensor and instrumentation technology as a viable design/upgrade option to provide improved plant stability, system reliability, and operational margins for safe and sustained operations**

- **This contribution to the technical basis for qualifying EDDs in regard to CCF vulnerability will benefit all reactor types, both existing and emerging**