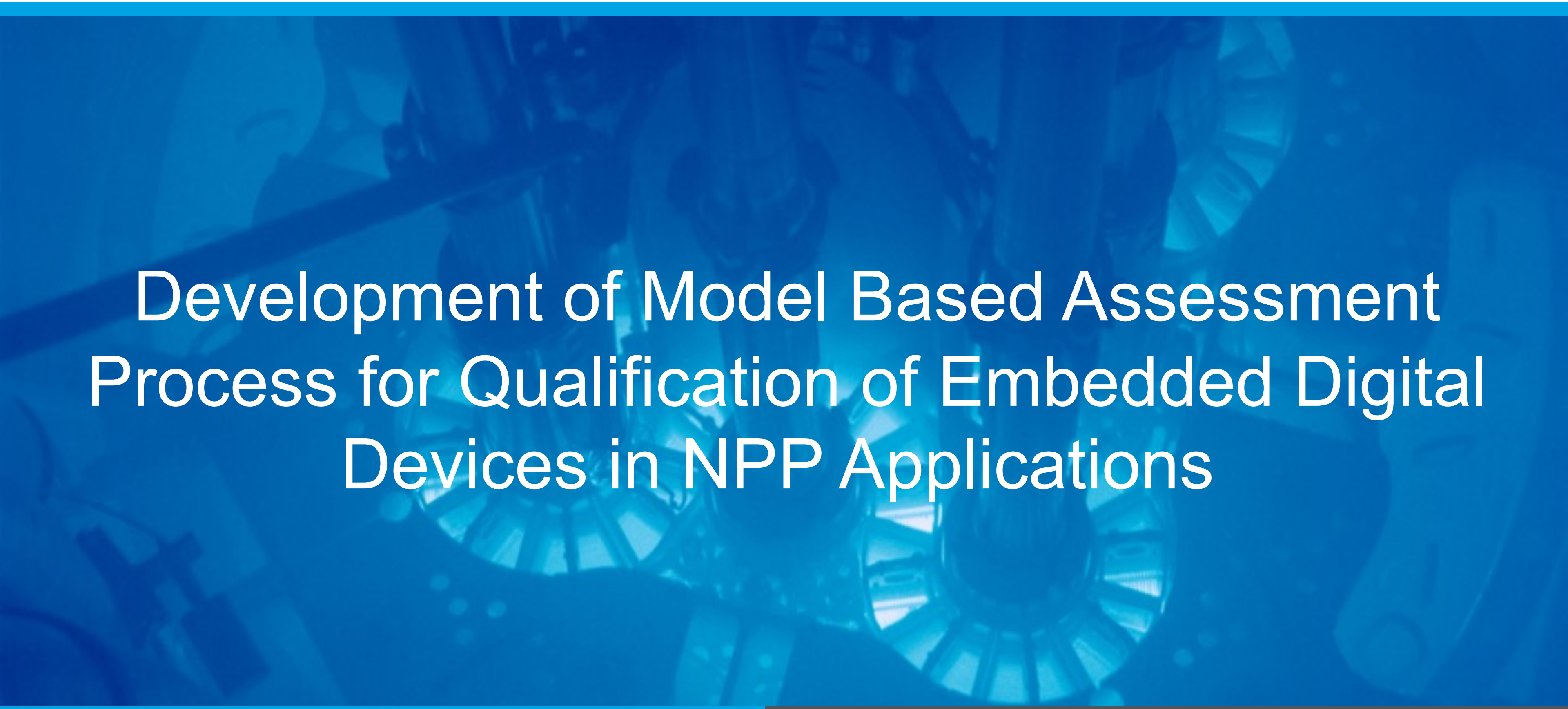
U.S. DEPARTMENT OF ENERGY | Office of NUCLEAR ENERGY

Clean. Reliable. Nuclear.



Development of Model Based Assessment Process for Qualification of Embedded Digital Devices in NPP Applications

Advanced Sensors and Instrumentation Annual Webinar

October 31 – November 1, 2018

Richard Wood
The University of Tennessee

Model-Based Testing for Qualification of EDDs

- **Project Goal and Objectives –** Development and demonstration of a systematic approach to assess whether instrumentation with an embedded digital device (EDD) is subject to software common–cause failure (CCF)
  - Define a classification scheme for EDDs to characterize their functional impact and facilitate a graded assessment approach
  - 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 a representative digital instrument
- **Schedule** – Currently completing testing and analysis → Final report to document results (project ends January 2019)

Participants on MBT for Qualification of EDDs Project

THE UNIVERSITY OF TENNESSEE KNOXVILLE

The University of Tennessee

- Richard Wood (2018)
- Tanner Jacobi (MS – 2018)
- Dan Floyd (BS – 2018)

THE OHIO STATE UNIVERSITY

The Ohio State University

- Carol Smidts (2018)
- Boyuan Li (2018)
- Xiaoxu Diao (2018)

AMS

Analysis Measurement Services

- Hashem Hashemian (2018)
- Brent Shumaker (2018)
- Alex Hashemian
- Kendrick Stiles (2018)
- Tyler Gavin (2018)
- Sam Caylor (2018)

VCU VIRGINIA COMMONWEALTH UNIVERSITY

Virginia Commonwealth University

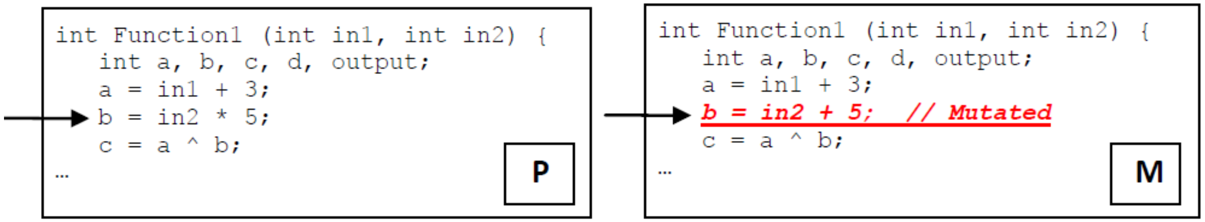
- Carl Elks (2018)
- Tim Bakker
- Frederick Derenthal (2018)
- Matthew Leccadito (2018)

Project Activities

- Development of the Model-Based Testing Framework – three-fold approach that includes:
  - Extension of the traditional mutation testing techniques to the requirements and design level
  - Development of a method to execute the specification documents in the requirements and design level
  - Development of an automate tool to generate test cases that can kill the mutants generated using the extended mutation testing approach
- Design and execution of experiment to demonstrate the effectiveness and efficiency of the MBT framework
  - Generation of demonstration artifact
  - MBT testing
  - Black-box baseline testing

Extension of traditional mutation testing techniques

- Traditional Mutation Testing
  - Mutation testing generates an effective test set
  - Mutation testing manipulates source code to generate mutants
  - An adequate test suite is able to distinguish (”kill”) all mutants
  - Traditional mutation testing focuses on the software code level and does not address requirements and design faults



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

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

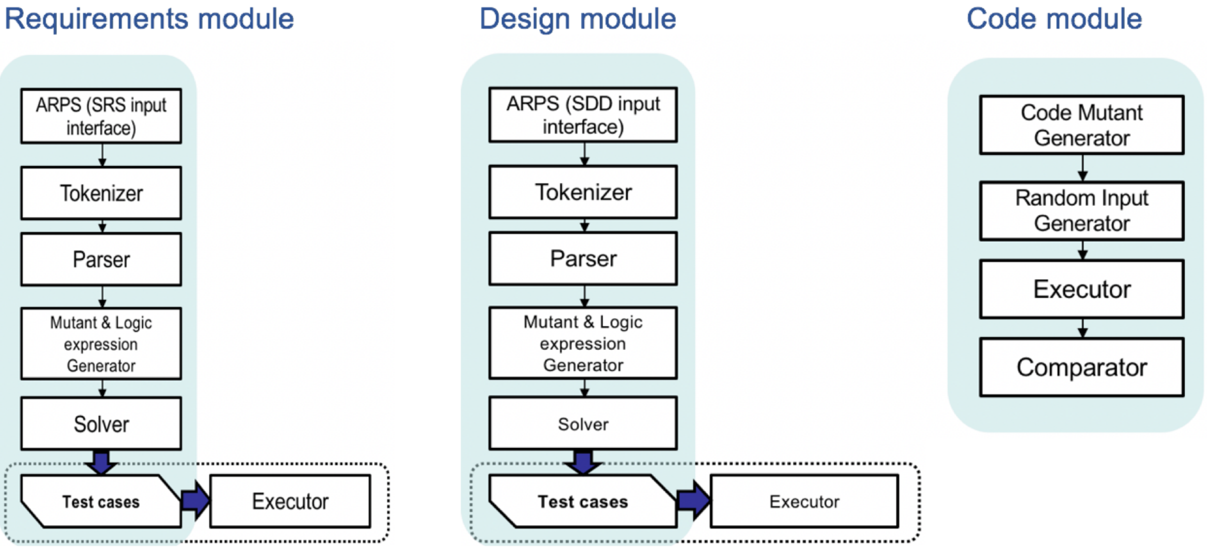
- Extension of the traditional mutation testing techniques includes:
  - Identification and classification of defects introduced in the requirements and design phase
  - Development of mutation operators for each defect category
  - Quantification of the number of mutants for each mutation operator
  - Development of a cost reduction strategy for each mutation operator

Treatment of Requirements and Design Defects

- Defects identification and classification
  - Traditional Mutation Testing uses mutation operators to systematically seed defects into the source code
  - To generate mutants at the requirements and design level, it is necessary to identify and classify the defect types
  - Twenty-nine defects were identified and classified based on the structure of software requirements specification (SRS) and software design document (SDD)
  - Example: “Missing Instance of Function”
    - Missing Instance of Function models the case where an occurrence of a specific function is missing from the logic specified in the SRS/SDD
- Executable model of the specification documents
  - SRS and SDD model enables generation and execution of mutants at the requirements and design level for software-based systems
  - Automated Reliability Prediction System (ARPS) is used to model the SRS and SDD using a High level Extended finite-state machine (HLEFSM)
  - Mutants can be generated by revising the HLEFSM

Automated Mutation Testing Tool (AMuTT)

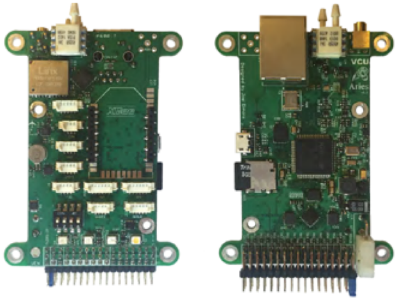
- An Automated Mutation Testing Tool (AMuTT) was developed to automates the test case generation process
- AMuTT includes 3 modules:
  - Requirements module
  - Design module
  - Code module



Experimental Demonstration of MBT Using Representative Instrument with an EDD

- Purpose
  - Demonstrate the efficacy of the MBT methodology on instrument with an EDD that is representative of commercial equipment
  - Proprietary concerns over IP → resulted in selection of VCU Smart Sensor

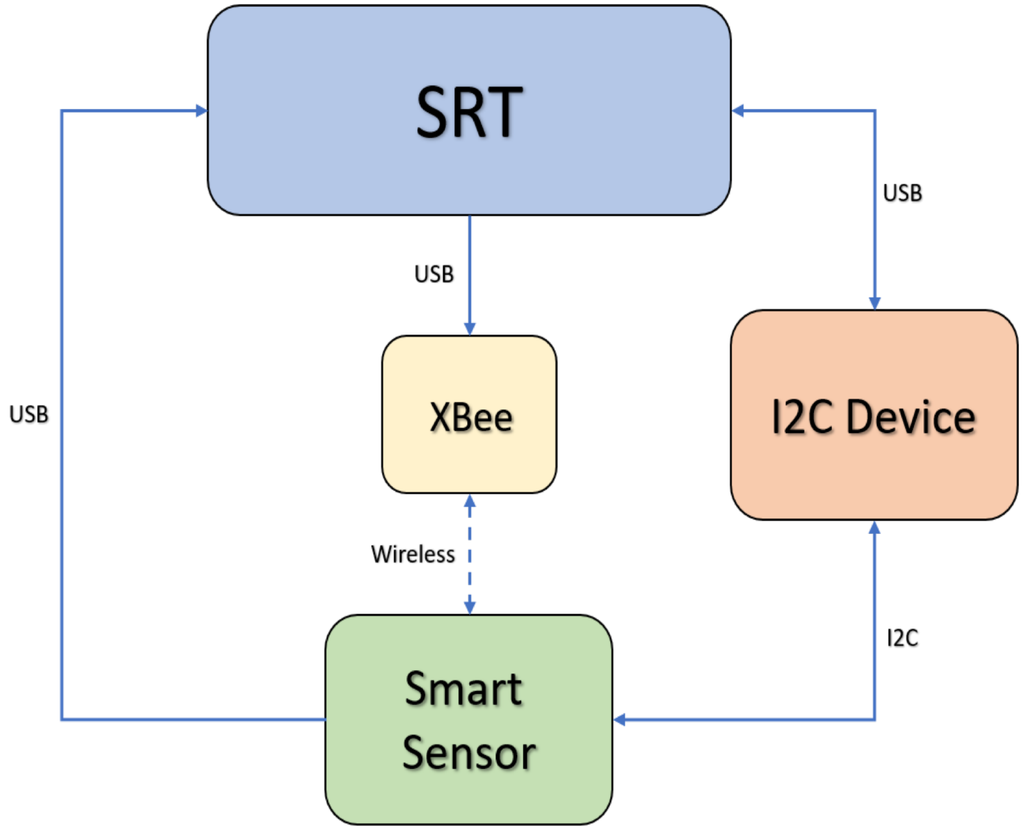
- VCU Smart Sensor
  - Derived from a Part-23 (non-safety-related) VCU ARIES_2 Advanced Autonomous Autopilot Platform
  - Barometric pressure and temperature measurement device
  - Software
    - Real-Time Operating System – ChibiOS
      - Deterministic real-time multi-threaded scheduling
    - HW Drivers – sensors, I2C, SPI, wireless, Ethernet
    - Communication layers for various high speed I/O
    - Device configuration, storage of calibration information, performance of sensor functions:
      - Re-ranging, transmitter calibration, averaging (first order Kalman filter, moving average filter)
      - Logging of data



Experimental demonstration of MBT

- Approach: Compare results of the MBT framework with the results of the black-box random testing baseline method
- The procedures followed in the experiment:
  - Develop the software under test (SUT)
    - VCU developed the software [The development of the SUT followed the waterfall model]
  - Creation of the SUT variants
    - VCU created 20 SUT variants by seeding defects into the SRS, SDD and Source Code.
  - Defects identification using the black-box baseline random testing method
    - AMS generated test cases using the black-box random testing baseline method to identify defects in the SUT variant
  - Defects identification using the MBT framework
    - OSU generated test cases using the MBT framework. The automation tool AMuTT was used to help generate test inputs in the requirements, design and code level. The test cases are being executed on the SUT variant to identify defects.

Black Box Baseline Testing



- Software Reliability Tester (SRT) provides automated black box testing
- Test cases input directly on the I2C bus
- Outputs compared with software model of the smart sensor
- Over 100k test cases per hour
- Confirmed ‘no-fault’ code showed no errors
- Tested 8 of 20 ‘faulted’ versions to date
- SRT detected errors in each of the 8 faulted builds

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

Conclusion

Status

- Demonstration of MBT effectiveness
  - Experimental testing nearing completion
  - Analysis of results underway

Accomplishments to date

- Extended mutation testing approach established
- Automated mutation testing tool developed to automate test generation process at the requirements, design, and code levels
- Classification approach for equipment with an EDD devised, including an extended approach to treat EDDs in D3 analyses
- VCU Smart Sensor hardware and software design now available as tool for research community

Outcome – The practical methods, tools, and demonstrations that results from this research effort will:

- Facilitate digital I&C qualification activities for advanced instrumentation technology to support deployment in the nuclear power industry
- Support reactor vendors and utilities in assessing I&C design and modernization options without substantial regulatory risk and implementation costs

Clean. Reliable. **Nuclear.**

Contact: **Richard Wood**

rwood11@utk.edu