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

Richard Wood
The University of Tennessee

NEET Project No.: 15-8097

October 12-13, 2016

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

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

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

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)

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Project Participants

The University of Tennessee

- Richard Wood
- Tanner Jacobi
- Dan Floyd

Analysis Measurement Services

- Hashem Hashemian
- Brent Shumaker
- Alex Hashemian

The Ohio State University

- Carol Smidts
- Boyuan Li

Virginia Commonwealth University

- Carl Elks
- Tim Bakker
- Frederick Derenthal

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Milestones Completed

M3CA-15-TN-UTK_-0703-031

- Evaluate current regulatory framework for assessing and treating CCF vulnerabilities: May 15

M2CA-15-TN-UTK_-0703-032

- Conduct and capture findings of workshop on CCF regulation and mitigation experience: July 25

M2CA-15-TN-UTK_-0703-033

- First 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

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Technical Accomplishments

Workshop on Qualification of Embedded Devices: March 11 in Bethesda

- Organized and conducted workshop with 6 invited speakers and +50 participants from industry, university, and government
- Captured technical insights and documented key findings

Regulatory Framework

- Investigated and documented the regulatory framework for addressing CCF vulnerabilities in digital I&C systems
- Captured the historical development of regulatory policy and guidance

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Technical Accomplishments

Equipment with Embedded Digital Devices

- Identified manufacturers of equipment with EDDs and equipment with EDDs currently installed in NPPs
- Investigated equipment to determine functional role of EDDs
- Engaged with manufacturers to solicit participation in project

CCF Evaluation Approach

- Developed a preliminary approach to systematically evaluate CCF vulnerability for equipment with EDDs
- Shared approach with industry for initial application in the D3 analysis for an advanced reactor

Technical Accomplishments

Mutation Testing

- Completed extensive review of traditional mutation testing (code level)
- Extended mutation testing approaches to address the requirements and design level of software life cycles

Testing and Evaluation

- Developed smart sensor prototype based on existing hardware and software to serve as testing target
- Evaluated two high-fidelity hardware simulators: Simics, OVPsim
- Developed an OVPsim platform based on the smart sensor prototype for future integration in the automated mutation-testing framework

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Mutation Provides Efficient Model-Based Approach to Software Testing

- **Mutation testing is model-based testing using mutants of the original code to qualify test data sets which can be used to find real faults**
- **Traditional mutation testing focuses on the software code level so extension required to address requirement and design faults**
- **Current research includes emphasis on reducing the high cost of mutation testing**
- **Existing code mutation cost reduction techniques include:**
  - Mutant Sampling
  - Mutant Clustering
  - Selective Mutation
  - Higher Order Mutation
  - Weak/Strong/Firm Mutation
  - Run-time Optimization

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Development of a Mutation Testing Framework

Defect and mutation operators- Examples

Defect category	Defect name and definition		Mutation Operator
Category 1: Defects for the definition of level 1 functions	Missing (definition of) function	The entire definition of a function is missing from the SRS/SDD.	MF
	Extra (definition of) function	The entire function definition is extraneous.	EF
	Incorrect/ambiguous function name	The name of the function is incorrect/ambiguous.	IAFN
	Function with incorrect logic	The functionality is valid but the logic is erroneous.	FIL
	Function with Incorrect functionality	The functionality is not valid.	FIF
Category 2: Defects related to inputs	Missing input	The definition of an input is missing from the SRS/SDD.	MI
	Extra input	The definition of an input is extraneous.	EI
	Incorrect/ambiguous input name	The name of the input is incorrect or ambiguous when it is defined	IAIN
	Input with incorrect type	The type of the input is erroneously defined.	IIT
	Input with incorrect range	The range of the input is erroneously defined.	IIR

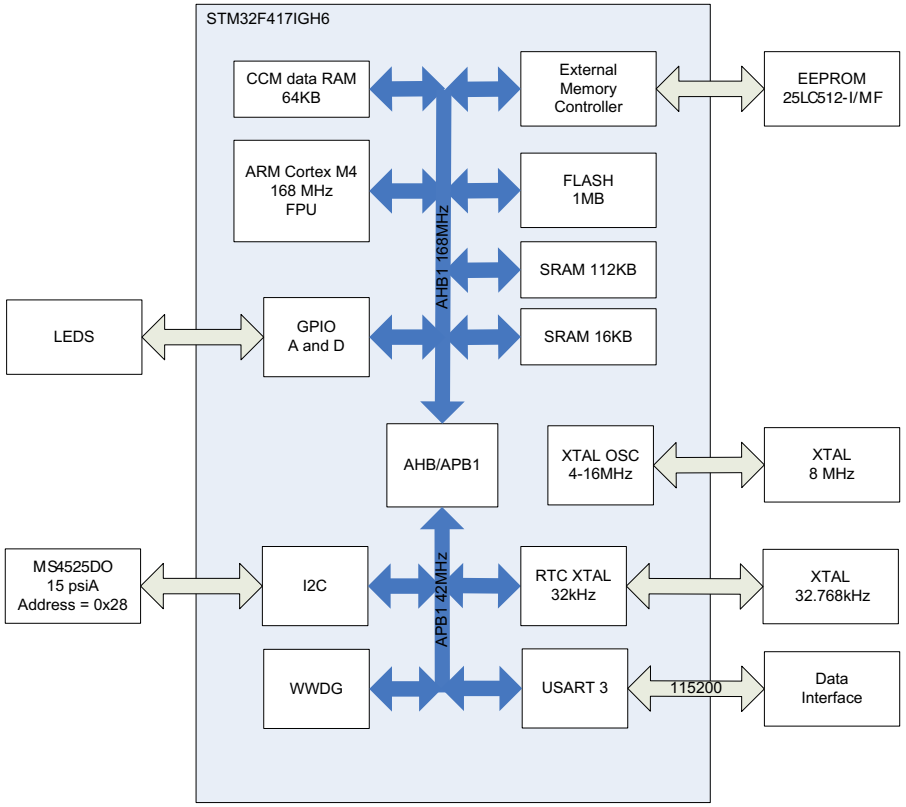
U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Virtual Platform Emulator of Smart Sensor Prototype

- **Developed as a representative benchmark to facilitate development of testing framework**
- **Pursuit of commercial smart device demonstration target continues**
- **Temperature and Pressure monitor**
  - Based on mature hardware and software developed by VCU
  - SW and HW design is representative in terms of form, function and complexity of avionics smart sensor.
  - Application code provides:
    - Calibration options
    - Output of measurements
  - Real-Time OS (ChibiOS)
    - Provides real-time scheduler
    - Hardware Abstraction

VCU Smart Sensor Architecture

Virtual Hardware Platform



U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Activities for Second Year

- **Conclude investigation of commercial equipment with EDDs**
  - Determine range of functionality that EDDs provide in equipment
  - Develop classification scheme based on functional role of EDD in performance of equipment
  - Continue interaction with equipment manufacturers to secure collaborating partner in testing and assessment of CCF potential
  - Select representative equipment with EDDs to serve as the demonstration target for testing

- **Development of the model-based testing methodology**
  - Generate and execute mutants for selected digital devices
  - Automate the mutation process
  - Finalize OVPsim Platform development
  - Develop and prototype an automated framework for model-based testing
  - Develop and prototype integrated mutation and fault injection methodology

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

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

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

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**

U.S. DEPARTMENT OF ENERGY

Nuclear Energy

Questions?