DEVELOPMENT OF A MODEL BASED ASSESSMENT PROCESS FOR QUALIFICATION OF EMBEDDED DIGITAL DEVICES IN NPP APPLICATIONS: RESEARCH APPROACH AND CURRENT STATUS

Richard Wood
The University of Tennessee
Knoxville, TN 37996-2300
woodrt@utk.edu

H.M. Hashemian
Brent Shumaker
AMS Corporation
Knoxville, TN 37923
hash@ams-corp.com
bshumaker@ams-corp.com

Carol Smidts
The Ohio State University
Columbus, OH 43210
smidts.1@osu.edu

Carl Elks
Virginia Commonwealth University
Richmond, VA 23284
crelks@vcu.edu

ABSTRACT

The instrumentation and control (I&C) equipment used in currently operating U.S. nuclear power plants (NPPs) is primarily based on mature analog technologies that are progressing towards obsolescence. The continued reliance on this legacy analog technology, which is also being propagated into new NPP designs, imposes performance penalties and maintenance burdens in comparison with modern digital I&C instrumentation. In many instances, currently available I&C equipment contain embedded digital devices (EDDs) such as microprocessors and programmable logic devices. Experience in other industries, such as avionics, has shown that digital I&C equipment containing EDDs can provide significant benefits over analog-based equipment in terms of performance, reliability, and maintainability. In recent years, due to the high demand for digital technologies in the industrial I&C marketplace, it is becoming increasingly difficult for NPPs to acquire instrumentation that is not equipped with an EDD. However, the nuclear power industry has been slow to adopt digital technology, especially in safety-related systems, in large part as a result of regulatory concerns about common-cause failure (CCF) vulnerabilities of equipment with EDDs. Consequently, there is a clear need to develop cost effective qualification methods to contribute to the assessment of CCF vulnerability posed by EDDs in modern instrumentation that could be used in NPPs.

This paper describes the research regarding qualification methods for equipment with EDDs that is sponsored by the Nuclear Energy Enabling Technologies (NEET) Advanced Sensors and Instrumentation (ASI) program of the U.S. Department of Energy (DOE). The purpose of the current research is to develop an effective approach employing science-based methods to resolve

concerns about CCF vulnerability that serve to inhibit deployment of advanced instrumentation (e.g., sensors, actuators, microcontrollers) with EDDs in nuclear power applications.

Key Words: embedded digital device, common-cause failure, mutation testing

1 INTRODUCTION

Much of the instrumentation and control (I&C) equipment in currently operating U.S. nuclear power plants (NPPs) is based on very mature, primarily analog technology that is steadily trending toward obsolescence. The continued reliance on this legacy analog technology, which is also being propagated into new NPP designs, imposes performance penalties and maintenance burdens in comparison with modern digital I&C instrumentation [1]. Experience in other industries has shown that digital technology can provide substantial benefits in terms of performance, reliability, and maintainability. Nevertheless, the nuclear power industry has been slow to adopt digital technology primarily because of regulatory uncertainty, implementation complexity, and limited availability of nuclear-qualified vendors and products. A specific concern is the potential for common-cause failure (CCF) vulnerability associated with embedded digital devices.

Given the great demand for digital functionality in high-volume industries, the industrial I&C marketplace is dominated by digital technology. In many instances, currently available I&C equipment contain embedded digital devices (EDDs) such as microprocessors and programmable logic devices. Consequentially, it is increasingly difficult to acquire instrumentation that is not equipped with an embedded digital device (EDD). These EDDs serve to enhance the performance, reliability, and flexibility of the equipment. However, the inclusion of an EDD also adds complexity to equipment functionality and increases the potential for latent systematic faults, which, in turn, complicates demonstration of qualification for safety-related applications. Without systematic, cost effective methods to resolve concerns about the qualification of digital technology, the nuclear power industry faces a significant challenge in modernizing its safety-related I&C equipment to address obsolescence and enhance performance.

This paper describes the research regarding qualification methods for equipment with EDDs that is sponsored by the Nuclear Energy Enabling Technologies (NEET) Advanced Sensors and Instrumentation (ASI) program of the U.S. Department of Energy (DOE). The purpose of the current research is to develop an effective approach employing science-based methods to resolve concerns about CCF vulnerability that serve to inhibit deployment of advanced instrumentation (e.g., sensors, actuators, microcontrollers) with EDDs in nuclear power applications. The research objectives address the challenge of establishing high levels of safety and reliability assurance needed for the qualification of EDDs (e.g., microprocessors, programmable logic devices) that are subject to software design faults, complex failure modes, and CCF vulnerability. Specific objectives are: (1) assess the regulatory context for treatment of CCF vulnerability in EDDs, (2) define a classification scheme for EDDs to characterize their functional impact and facilitate a graded approach to their qualification, (3) develop and extend model-based testing methods to enable effective demonstration of whether devices are subject to CCF, which may arise from vulnerabilities introduced at any stage of the design lifecycle, (4) establish a cost-effective testing framework that incorporates automation and test scenario prioritization, and (5) demonstrate the qualification approach through selection and testing of candidate digital device(s).

In the first phase of the research, a workshop was held among nuclear energy stakeholders to discuss regulatory and technical challenges, recent experience, and emerging approaches. As part of an effort to understand the context and extent of the challenge, the current regulatory framework for treating CCF vulnerabilities in digital I&C was evaluated and survey was conducted of current instrumentation products to identify usage of EDDs. To develop the basis for a systematic approach to model-based testing, current software engineering techniques for mutation testing were investigated and extended to address requirement and design phases of the software life cycle in addition to coding. In addition, initial

development of a cost-effective testing framework focused on automated generation of mutant operators, establishment of a hardware simulator platform, and adoption of a smart sensor prototype to serve as an initial basis for developing the testing framework. The progress and findings from some of these activities is summarized in this paper. Other papers have been generated to document additional findings from this phase of project activity and related work [2–5].

2 PROJECT OVERVIEW

As part of its cross-cutting research to address technology needs and challenges that affect the continued availability of nuclear energy, the DOE NEET ASI program established a research project involving the University of Tennessee, The Ohio State University, Virginia Commonwealth University, and Analysis and Measurement Services (AMS) Corporation. The project entitled, "Development and Demonstration of a Model Based Assessment Approach for Qualification of Embedded Digital Devices in Nuclear Power Applications," involves development of an approach employing model-based testing to help resolve concerns about CCF vulnerability. An effective demonstration of qualification can minimize uncertainties that serve to inhibit deployment of advanced instrumentation (e.g., sensors, actuators, microcontrollers) with EDDs in nuclear power applications.

The research objectives of the project address the challenge of establishing high levels of safety and reliability assurance needed for the qualification of EDDs (e.g., microprocessors, programmable logic devices) that are subject to software design faults, complex failure modes, and CCF vulnerability. Specific objectives are: (1) assess the regulatory context for treatment of CCF vulnerability in embedded digital devices, (2) define a classification scheme for equipment with an EDD to characterize its functional impact and facilitate a graded approach to qualification, (3) develop and extend model-based testing methods to enable effective demonstration of whether devices are subject to CCF, which may arise from vulnerabilities introduced at any stage of the design lifecycle, (4) establish a cost-effective testing framework that incorporates automation and test scenario prioritization, and (5) demonstrate the qualification approach through selection and testing of candidate digital device(s).

The subsequent sections describe the current status of the project, provide a brief explanation of the model-based testing approach being developed, and present a summary of key findings from industry engagement through a workshop.

3 PROJECT STATUS

The first year of research focused on establishing the context for treating qualification of equipment with an EDD and developing technical basis for model-based testing. In addition to conducting the workshop described below, initial research activity-involved evaluation of the regulatory framework for addressing CCF vulnerabilities in digital I&C systems, including capturing the historical development of regulatory policy and guidance. Concurrently, surveys of instrument vendors were conducted to determine the types of equipment on the market and the functional role assigned to the EDDs [2]. This information feeds into an effort to devise a classification approach, which has resulted in development of preliminary approach to systematically evaluate the potential impact of prospective CCF vulnerability for equipment with an EDD [3].

The fundamental technical development underway for this research involves establishment of a cost-effective qualification framework that incorporates model-based testing to support determination of whether equipment with an EDD is vulnerable to CCF. The approach for model-based testing has been generated, a suitable prototype intelligent device has been devised and emulated in a simulation environment, and the basic elements of a testing environment have been developed.

The model-based testing methodology under development is based on an extension of a software testing technique known as mutation testing. In this approach, tests are developed based on hypothesized

software faults arising from requirements, design, and coding sources. The objective is to define a test suite that can differentiate/detect the potential existence of each postulated fault. Mutation operators systematically seed faults in the base software, and the test suite is executed on the mutants (faulted software) to determine if the tests are sufficiently comprehensive to detect all of the seeded faults. The mutation testing framework provides a means to demonstrate that the full range of postulated faults are covered and thereby give evidence for the qualification of the software-based device.

As a development and demonstration target for the model-based testing methodology, an intelligent instrument was identified based on a prototype smart sensor. To facilitate software-based testing, a virtual platform emulator has been developed in the OVPSim simulation environment. Fig. 1 illustrates the testing framework [4] in which mutants are generated, introduced into the virtual platform simulator for automated testing, and the test results are analyzed to optimize the test cases and ensure all faults are detected by the test suite.

Ongoing research activities involve integrating the elements of the testing framework, incorporating automation and optimization techniques throughout the testing framework, and demonstrating the capabilities of model-based testing using the prototype smart sensor.

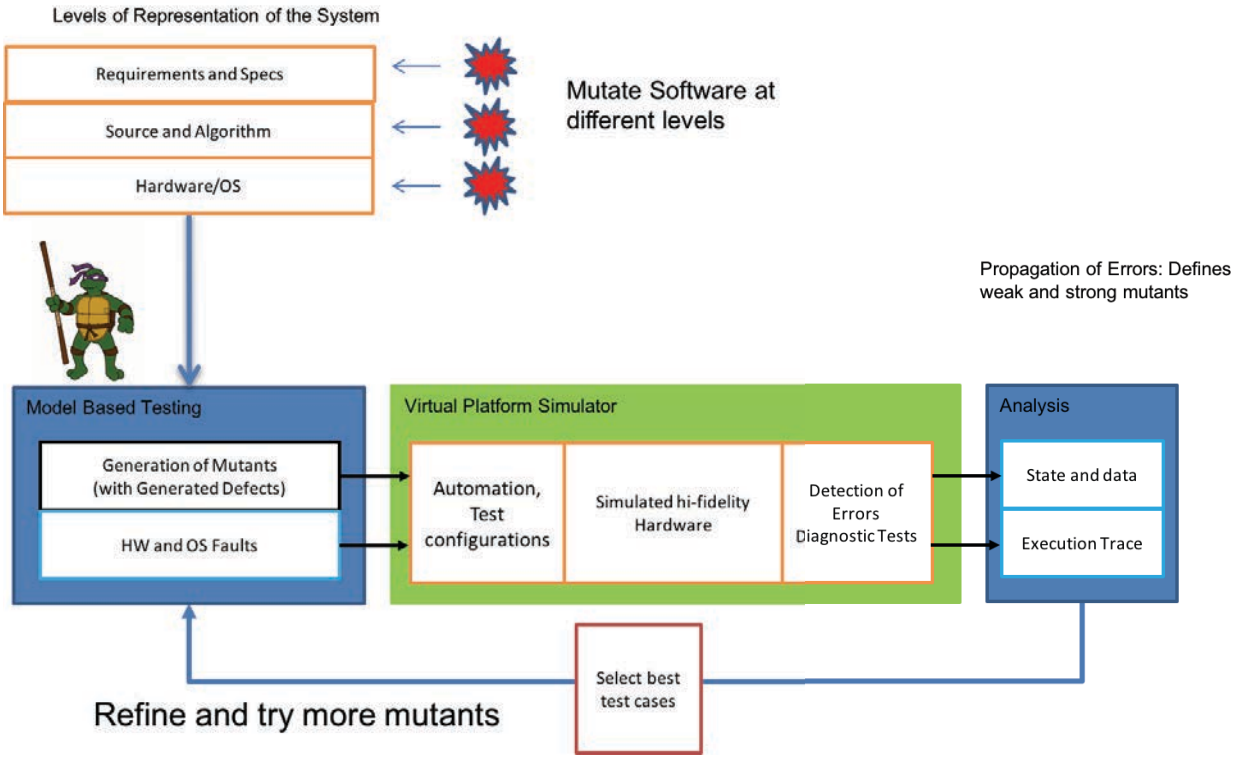


Fig. 1. Virtualized testing framework: simplified view.

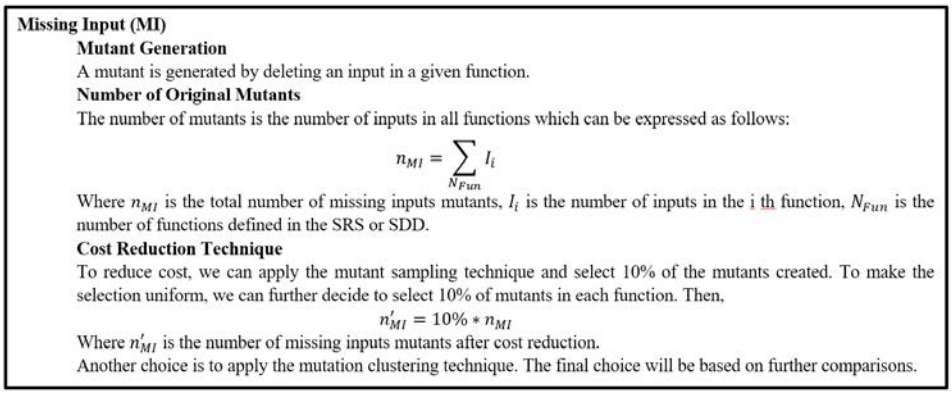
4! MODEL-BASED TESTING USING MUTATION OPERATORS

Mutation testing is a fault–based software testing technique that is considered to be the most efficient in detecting faults. It follows a set of rules which are called mutation operators to systematically seed faults into the source code. Each seeded fault results in a new version of the software, which is called a

mutant. Test suites are then developed to distinguish the mutants from the original program. The test suites are considered to be capable of detecting all indigenous faults if the test suite can find all the seeded faults. To reduce the high cost of mutation testing, various cost reduction techniques have been developed including Mutant Sampling, Mutant Clustering, Selective Mutation, etc.

Traditional mutation testing focuses on the software code level and promises to be effective in identifying adequate test data which can be used to find faults in the source code. However, traditional mutation testing is not geared towards the detection of requirements and design faults. To cover the full spectrum of possible faults, the research team has extended the mutation framework from the code level to the requirements and design level [5].

Twenty-nine defects that appear in requirements and design documents were identified to define appropriate mutants. Then corresponding mutation operators that model the defects were developed. For each mutation operator, the strategy to generate a mutant and the evaluation of the number of possible mutants were developed. Existing code level cost reduction techniques were tailored for requirements and design mutation operators that result in a large number of mutants. With the extended mutation testing framework, the full spectrum of possible faults will be tested and identified to ensure the safety and functionality of the software. The example of the mutation operator MI modeling the defect "Missing Input" is given in Fig. 2.



Missing Input (MI)

Mutant Generation

A mutant is generated by deleting an input in a given function.

Number of Original Mutants

The number of mutants is the number of inputs in all functions which can be expressed as follows:

$$n_{MI} = \sum_{N_{Fun}} I_i$$

Where n_{MI} is the total number of missing inputs mutants, I_i is the number of inputs in the i th function, N_{Fun} is the number of functions defined in the SRS or SDD.

Cost Reduction Technique

To reduce cost, we can apply the mutant sampling technique and select 10% of the mutants created. To make the selection uniform, we can further decide to select 10% of mutants in each function. Then,

$$n'_{MI} = 10\% * n_{MI}$$

Where n'_{MI} is the number of missing inputs mutants after cost reduction.

Another choice is to apply the mutation clustering technique. The final choice will be based on further comparisons.

Fig. 2. Example of a mutation operator.

5 CONCLUSIONS

This research conducted under this project will advance the state of the art in the qualification of advanced instrumentation with embedded digital devices for NPP application by (1) developing novel methods for establishing acceptable proof of operational reliability, (2) applying the developed methods to representative embedded digital devices to ascertain the effectiveness of the methodology, and (3) establishing a cost-effective qualification framework that is compliant to existing guidance and standards. The outcomes of this research will contribute substantially to the technical basis for qualifying embedded digital devices in regard to CCF vulnerability. The results will benefit all reactor types by resolving a current impediment to more extensive application of digital devices.

6 ACKNOWLEDGMENTS

This material herein is based upon work supported by the U.S. Department of Energy, Office of Nuclear Energy, under the Nuclear Energy Enabling Technology (NEET) Advanced Sensors and Instrumentation (ASI) Program. The authors would like to acknowledge Suibel Schuppner, the DOE NEET ASI program manager, for her oversight and assistance on this project. This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

7 REFERENCES

1. E. Quinn, J. Mauck, and K. Thomas, *Digital Technology Qualification Task 2 – Suitability of Digital Alternatives to Analog Sensors and Actuators*, INL/EXT-12-27215, Idaho National Laboratory, Idaho Falls, ID, 2012.
2. T. Jacobi et al, "Investigation of Instrumentation Containing an Embedded Digital Device," *Proc. of NPIC&HMIT 2017*, San Francisco, CA, June 11-15 (2017).
3. R. Wood, J. Mauck, and E. Quinn, "Addressing Embedded Digital Devices in Safety-Related Systems of Nuclear Power Plants," *Proc. of NPIC&HMIT 2017*, San Francisco, CA, June 11-15 (2017).
4. Frederick Derenthal, Carl Elks, Tim Bakker, Mohammadbagher Fotouhi, "Virtualized Hardware Environments for Supporting Digital I&C Verification," *Proc. of NPIC&HMIT 2017*, San Francisco, CA, June 11-15 (2017).
5. Boyuan Li and Carol Smidts, "Extension of Mutation Testing for the Requirements and Design Faults," *Proc. of NPIC&HMIT 2017*, San Francisco, CA, June 11-15 (2017).