A Statistical Testing Approach for Quantifying Software Reliability: Application to an Example System

Tsong-Lun Chu, Athi Varuttamaseni, Joo-Seok Baek

2016 ANS Winter Conference
Las Vegas, NV

November 2016

Nuclear Science and Technology Department
Brookhaven National Laboratory

U.S. Department of Energy
Office Of Science
American Nuclear Society

Notice: This manuscript has been authored by employees of Brookhaven Science Associates, LLC under Contract No. DE-SC0012704 with the U.S. Department of Energy. The publisher by accepting the manuscript for publication acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes.
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, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or any third party’s use or the results of such use 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 or its contractors or subcontractors. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.
A Statistical Testing Approach for Quantifying Software Reliability; Application to an Example System

Tsong-Lun Chu, Athi Varuttamaseni, and Joo-Seok Baek

Brookhaven National Laboratory, 33 N. Renaissance Road, Upton, NY 11973, chu@bnl.gov

I. INTRODUCTION

The U.S. Nuclear Regulatory Commission (NRC) encourages the use of probabilistic risk assessment (PRA) technology in all regulatory matters, to the extent supported by the state-of-the-art in PRA methods and data. Although much has been accomplished in the area of risk-informed regulation, risk assessment for digital systems has not been fully developed. The NRC established a plan for research on digital systems to identify and develop methods, analytical tools, and regulatory guidance for (1) including models of digital systems in the PRA’s of nuclear power plants (NPPs), and, (2) incorporating digital systems in the NRC’s risk-informed licensing and oversight activities.

Under NRC’s sponsorship, Brookhaven National Laboratory (BNL) explored approaches for addressing the failures of digital instrumentation and control (I&C) systems in the current NPP PRA framework. Specific areas investigated included PRA modeling digital hardware, development of a philosophical basis for defining software failure, and identification of desirable attributes of quantitative software reliability methods. Based on the earlier research, statistical testing is considered a promising method for quantifying software reliability.

It is widely recognized that software failures are due to the triggering of pre-existing defects by the software’s operational environment. Software defects can arise from errors made in user requirements or coding errors introduced during the developmental process. The software’s operational environment includes factors such as the time history of digital system inputs, communication interfaces, the internal state of the digital system, and external conditions. Thus, software reliability is a function of both the number of pre-existing defects and the presence of a triggering condition caused by the manner in which the software is used.

In this paper, we describe a statistical software-testing approach for quantifying software reliability and applied it to the loop-operating control system (LOCS) of an experimental loop of the Advanced Test Reactor (ATR) at Idaho National Laboratory (INL). The work involved collaboration between BNL and INL.

The objectives of the study include:

1. Development of a statistical testing approach for estimating software failure probability on demand, the results of which are suitable for including in a probabilistic risk assessment (PRA); and,

2. Application of the approach to the LOCS to estimate its failure probability, and obtain insights into the feasibility, practicality, and usefulness of the estimation in models of digital systems for inclusion in nuclear power plants’ PRAs.

II. SUMMARY OF THE STATISTICAL TESTING APPROACH

The research described in this paper utilizes a statistical testing method (STM) to represent the operational environment and test the software to determine if this environment is capable of triggering pre-existing defects. The test results (number of failures) thus represent operational software failures. Since digital I&C systems (including the software) will be modeled in the NPP PRA sequences, the ways in which the digital system is used will be determined by each PRA sequence. For instance, if one postulated that the digital reactor protection system (RPS) appears in both the primary loss of coolant accident and steam generator tube rupture sequences, the inputs to this RPS and its software (such as the reactor’s temperature, pressure, steam-generator’s level, steam pressure) would follow different patterns, and different parts of the RPS software would be challenged; consequently, the probability of RPS failure might differ for each sequence. The STM method developed in this research produces test scenarios specific to each sequence and tests the RPS system against these scenarios to generate the sequence-specific probability of software failure.

The STM method consists of the following steps, which assumes that a PRA and an appropriate thermal-hydraulic model have been developed:

1. Select a system under test (SUT);
2. Identify SUT-related PRA sequences (represented by the cutsets);
3. Determine the thermal-hydraulic simulation boundary conditions corresponding to the selected cutsets;
4. Run the thermal-hydraulic model to calculate a time history of the reactor and the plant physical conditions.
   Such outputs are test scenarios to the SUT;
5. Execute test scenarios and collect test results; and,
6. Analyze the test results to quantify the probability of software failure.

III. APPLICATION TO AN EXAMPLE SYSTEM

In this study, BNL selected a Loop Operating Control System (LOCS) for the ATR at INL as the SUT. The ATR has six in-pile tubes (IPTs) through which water circulates at a set pressure, temperature, and flow rate. The LOCS normally controls the condition of an experimental loop, and will generate a reactor trip signal when the pressure, temperature or flow exceeds its threshold. Figure 1 shows the logic involved for the IPT inlet’s temperature-protection channel. It illustrates how the different protective functions are logically connected to each other via an OR gate. Hence, regardless of the channels that initiate the trip, the three digital output-modules normally should be in the same state (i.e., the status of all three should show either a trip or non-trip).

The authors acknowledge the collaboration of INL staff on the research and the participation of the NRC project manager.

REFERENCES


---

**Fig. 1** Typical processing logic of the loop-protective channel

**Fig. 2** Work flow associated with performing the tests
<table>
<thead>
<tr>
<th>No.</th>
<th>Failure Effect Category</th>
<th>Subcategory [Frequency of Subcategory]</th>
<th>Parameter Description</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Loss of HX cooling</td>
<td>-</td>
<td>Time at which the heat transfer coefficient reaches zero. [s]</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>Pump Failure</td>
<td>Trip [49%]</td>
<td>Multiplication constant to the time variable for the pump’s coastdown curve</td>
<td>0.5</td>
</tr>
<tr>
<td>3</td>
<td>Seizure [51%]</td>
<td>Time for pump to reach complete stop [s]</td>
<td></td>
<td>0.001</td>
</tr>
<tr>
<td>4</td>
<td>Pipe Plugging</td>
<td>Plugging at FE1 [33.3%]</td>
<td>Flow area at junction 855 [ft²]</td>
<td>1.00E-08</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>Plugging at FE2 [33.3%]</td>
<td>Flow area at junction 856 [ft²]</td>
<td>1.00E-08</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>Plugging at S145 [33.4%]</td>
<td>Flow area at junction 857 [ft²]</td>
<td>1.00E-08</td>
</tr>
<tr>
<td>7</td>
<td>Pipe Break</td>
<td>Break at IPT Inlet [50%]</td>
<td>Flow area at valve 851 [ft²]</td>
<td>6.3840E-06</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>Break at IPT Outlet [50%]</td>
<td>Flow area at valve 853 [ft²]</td>
<td>6.1500E-06</td>
</tr>
<tr>
<td>9</td>
<td>Loss of flow control - input</td>
<td>CV-240 (Flow sensor input) [gpm]</td>
<td></td>
<td>30.06</td>
</tr>
<tr>
<td>10</td>
<td>Loss of flow control - output</td>
<td>CV-24 (Flow controller output) [flow area ratio]</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>Loss of line heater control – input</td>
<td>CV-1 (490°F - Temperature sensor input) [°F]</td>
<td></td>
<td>45</td>
</tr>
<tr>
<td>12</td>
<td>Loss of line heater control – output</td>
<td>CV-4 (Line heater controller output) [W]</td>
<td></td>
<td>1.799637E+05</td>
</tr>
<tr>
<td>13</td>
<td>Loss of TCV control</td>
<td>Time for valve TCV-3-1 to be fully closed. [s]</td>
<td></td>
<td>15</td>
</tr>
</tbody>
</table>