A CATHENA-Based Approach To The Development Of Shutdown System Reliability Test Profiles

J.S. Baxter, A. Ranger, V. Lau, M. Chan, J. Ballyk and A. McDonald
Atomic Energy of Canada Limited, Mississauga, Ontario, Canada

Abstract

Reliability testing is a statistical means of safety-critical software qualification, in which inputs are simultaneously varied, and outputs checked against functional requirements. The test developers balance the need for realistic event scenarios and trip coverage completeness with the randomness and large number of test cases required for statistical validity.

The need for realistic event scenarios and trip coverage completeness is met through use of the Canadian Algorithm for Thermalhydraulic Network Analysis (CATHENA) as a basis for test profile generation. The CATHENA-based approach ensures realistic scenarios and adequate coverage by starting with the analysis models. The developer converts the output file from each CATHENA run into a baseline profile, which is a text file containing a series of time-stamped trip computer input values representing the event scenario.

The test developer then converts the baseline profiles into 10,000 test profiles by applying noise and other random effects to each signal.

1. Introduction

1.1 Objective

AECL has used several methods of plant modeling to support reliability qualification of the shutdown system trip computer software. Our most recent development is to use the extensive plant modeling and analysis capabilities of CATHENA to produce the simulated upset conditions required for reliability testing of the shutdown system trip computers.

1.2 Shutdown System Computers in CANDU 6 Design

The CANDU 6 design has two independent shutdown systems, each of which is capable of shutting down the reactor in the event of a serious process excursion. Process parameters and reactor power signals are monitored by trip computers. The computers and associated instruments are triplicated and grouped into channels with relay-based voting logic so that a single computer failure will neither result in a system failure nor cause a reactor trip. At least two out of three channels must trip before the voting logic will trigger a reactor trip.

The trip computers monitor process signals, such as Primary Heat Transport System (PHT) flows and pressures and the Steam Generator level. The trip computers also monitor the reactor power signals to determine power-dependent setpoints and conditioning levels for the process parameter trips. The reactor power signals are therefore within scope of reliability testing insofar as they contribute to the process parameter trip decision.

The reactor power trip parameters, such as high neutron overpower and high log rate are implemented using analog comparators instead of computers, and are not within scope of software reliability testing.

1.3 Overview of Reliability Testing

An important and still developing aspect of software testing is the measurement of software reliability. The measurement is done by performing a statistically significant number of independent random tests on the software. Testing continues until the software has passed enough tests to establish the desired limit on the probability of a random software failure.

Each test profile for a random test of the shutdown system trip computer software consists of a unique set of time-stamped plant parameter values representing the input signals received by the trip computer during a plant event or accident. Ideally, each test profile begins with signals simulating the plant under various normal operating conditions, continues with test signals simulating a plant event or accident, and ends with signals requiring a trip signal from the shutdown system software.

In the CATHENA-based approach, the test profiles are created as random perturbations to a set of baseline profiles. Each baseline profile represents the plant response to a particular class of event as modeled for safety analysis.

During reliability qualification, AECL tests that the trip computer software responds as specified to 10,000 unique test profiles, thereby demonstrating with an acceptable level of confidence that the software has met the reliability target of 0.9999 ($1\text{-}10^{-4}$) as the probability of a correct software response on demand.

2. Components of Reliability Testing

2.1 Statistical Basis

The response of the trip computer under test to simulated accident conditions is interpreted as a Bernoulli trial – one of a series of independent tests, each with two possible outcomes. If the trip computer response is consistent with the trip computer functional requirements, then the trial is successful. The software reliability is interpreted as the probability q that the trip computer will respond as specified to a trip condition. The software unreliability or failure rate is the probability p (equal to $1\text{-}q$) that the software will not respond as specified.

The binomial distribution is an accepted model for large numbers of Bernoulli trials. If n Bernoulli trials are held, and the probability of success in a single trial is q, then the binomial distribution gives the expected number of successes N as in Equation 1.

$$N = q \times n \tag{1}$$

The probability $P(N)$ that exactly N successes will result from n trials (where $N \leq n$) is shown in Equation 2.

$$P(N) = q^N \times p^{n-N} \tag{2}$$

The probability $P(n)$ that n successes (or zero failures) will be detected is shown in Equation 3 by rewriting Equation 2 with N equal to n.

$$P(n) = q^n \tag{3}$$

The probability $P(n)$ in Equation 3 is interpreted as one minus the level of confidence α attained in a lower bound on q when zero failures are detected in a series of n tests. This is shown in Equation 4.

$$q^n \geq (1 - \alpha) \tag{4}$$

If the specified lower limit on q is defined as Q, then the inequality in Equation 4 can be removed as per Equation 5.

$$\alpha = 1 - Q^n \tag{5}$$

Equation 5 is arranged in Equation 6 to show the minimum number of tests required to attain a desired level of confidence that $q \geq Q$.

$$n = \log(1-\alpha) \div \log(Q) \tag{6}$$

According to Equation 6, a quantity of 6932 independent tests are required to demonstrate a 0.9999 lower bound on the trip computer software reliability with a confidence level of 50%.

It is important to clarify that a confidence level does not imply a 50% likelihood of software failure. It does imply that there is a 50% probability that exactly 6932 tests will establish the minimum software reliability target of 0.9999.

The preceding argument can be illustrated by first assuming that the trip computer software reliability is exactly 0.9999. If 6932 trip conditions are simulated, the probability that the trip computer will respond as specified to every simulated trip condition (i.e., the probability of zero failures) is given as 0.5000 by Equation 3. This implies that if the complete set of 6932 tests were performed over and over again, zero failures would be detected 50% of the time. Therefore performing a set of 6932 tests once and detecting no failures gives 50% confidence that the lower limit of 0.9999 on the software reliability has been met.

Therefore, reliability testing requires that at least 6932 trip conditions be simulated as independent tests, and that the trip computer software under test respond as specified to every one. The minimum requirements are exceeded by simulating 10,000 trip conditions.

2.2 Test Platform Development and Verification

The test platform hardware consists of a test computer with its inputs and outputs connected to the trip computer outputs and inputs respectively, and standard user interface hardware allowing the tester to inject trip computer input signals, such as test profiles, and monitor the trip computer responses through the output signals.

The test platform software consists of a test script interpreter and a test oracle. The interpreter reads the test instructions from the user interface or from a text file, interprets the instructions, transmits simulated field signals to the trip computer, monitors the trip computer output signals, and logs the results for offline analysis.

The test oracle software is essentially a virtual trip computer. It models the trip computer logic per the functional specifications, excluding hardware-dependent functions such as self-checks and restart logic. Its purpose is to predict the output values of the trip computer in response to the simulated event scenarios contained in the test profiles.

2.3 Generation of Test Profiles

The 10,000 test profiles to be applied to the trip computers undergoing reliability testing are generated before the start of testing and stored in individual text files for review and archival purposes. Offline production of test profiles allows complex plant modeling software, such as CATHENA, to be run without the constraint of real-time operation. It also permits review of the profiles prior to testing, and improves repeatability of the tests.

The duration of the test profile depends on the accident scenario and the trip parameter designed to protect against it. Typical durations are roughly ten seconds, but some event scenarios must last for three minutes before the profile exceeds a setpoint that requires the trip computer to trip.

2.4 Execution of Tests

An automatic test script is used to transmit the test input profiles and check the resulting outputs against the values predicted by the oracle.

The sequence of test actions is as follows:

- The script initializes the trip computer inputs to nominal, non-trip values and checks that the outputs are at the corresponding values.
- The script loads the selected test profile into the test platform memory, and transmits the initial value of the input signals to the trip computer and the test oracle.
- The script compares the initial trip computer output values with the values predicted by the oracle, and logs any discrepancies for offline analysis. Additional data are logged to assist in the analysis of any discrepancies.
- The script runs the test profile, sending each time-stamped set of input signal values to the trip computer and to the oracle in real time.
- The script stops sending new input signal values at the end of the test profile.
- The script compares the final trip computer output values with the values predicted by the oracle. The test platform maintains the trip computer input signals at the final values in the test profile while the comparison is made. The script flags any discrepancies for offline analysis, and logs additional data to assist in the analysis of any discrepancies.
- The script sets the input signals back to the nominal, non-trip values and freezes them until any delayed trips have had time to clear, thereby preserving the independence of each trial.
- The script proceeds to the next test profile.

2.5 Analysis of Mismatches

Discrepancies between the test oracle outputs and the trip computer outputs are analysed to confirm that the trip computer response was consistent with the functional requirements. Individual tests may be repeated if the discrepancy was due to a test rig hardware failure, and hence not attributable to a deficiency in the trip computer software.

The most common type of mismatches previously experienced is “chattering”, when an input signal in the test profile terminates extremely close to a trip or alarm setpoint. The test oracle receives the input signals through internal memory buffers, while the trip computer receives input signals through an I/O frame and is affected by noise. Reasonable effort is made during test profile development to ensure that most inputs signal profiles terminate beyond the setpoints by acceptable margins even after the addition of random noise effects.

Additional data logging instructions are included in the test script as an aid to offline, manual analysis of test results. The script records the values of input signals to help the tester identify signals that are near their setpoints, and may have led to chattering during the test.

3. Previous Approaches to Profile Generation

Earlier approaches to reliability testing made use of parameter-based mathematical models with the addition of random noise. Input signals were calculated as linear extrapolations from the nominal value to the trip value with minimal modeling of direct plant relationships between different signals. Such an approach had the advantages of speed and simplicity, but the profiles did not account for the dynamic relationships between parameters in a realistic plant model.

A more sophisticated approach involved individual generation of test profiles through a modified version of an earlier plant analysis software tool. The profiles were highly randomized and covered a large proportion of the signal space, but were subject to chattering as described above, and did not consistently terminate at signal values requiring trip computer action [1]. As a result, the test logs required extensive analysis and additional testing to ensure that the reliability objectives had been achieved.

4. CATHENA-Based Approach to Profile Generation

The CATHENA-based approach to reliability test profile generation under development at AECL, combines the best characteristics of the previous approaches. A modern thermodynamic code is used to ensure that the test profiles are consistent with the analysis basis of the trip parameter functional design. Simulated signal noise and other random effects are applied to increase the proportion of the signal space that is covered while ensuring that test profiles terminate with a computer trip demand value.

Table 1 lists the plant events analysed using the CATHENA software as the basis for reliability test profile generation, and Figure 1 illustrates the process by which the analysis output files are used in the generation of reliability test profiles.

4.1 Overview of CATHENA Analysis Code

CATHENA is a two-fluid thermal hydraulic computer code, developed by AECL for analysis of flow transients in reactors and piping networks [2]. It was designed to be as general as possible. CATHENA has been applied to the simulation of a wide range of thermal hydraulic problems, from test facilities (e.g., RD-14, CWIT, LOBI, etc.) to small-reactor systems (e.g., SLOWPOKE, MAPLE) to CANDU 6 thermal hydraulic accident analysis.

4.2 Selection of Analysis Events

The CATHENA-based approach to reliability test profile generation ensures realistic and adequate scenarios and trip coverage by using verified plant and event models that are prepared for safety analysis and modified for test profile generation.

Table 1 lists the existing CATHENA event models that are modified to save the plant parameters monitored by the trip computers, and the trip parameters that guard against each event.

Plant Event and Analysis Description	Trip Parameters	Events
Large LOCA • Two simulations with different break sizes and locations • Covers pump suction • Covers header break	PHT Low Pressure Pressurizer Low Level PHT Flow (SDS1) PHT ΔP (SDS2)	2
Loss of Class IV power • Two simulations at different reactor power levels • Covers various PHT upset cases	PHT High Pressure PHT Flow (SDS1) PHT ΔP (SDS2)	2
Various moderator upset cases	Moderator Low Level Moderator High Temp Moderator Pump ΔP	3
Secondary side events • LCV closure (two simulations at different reactor power levels) • Loss of feedwater flow (two simulations at different reactor power levels)	Boiler Low Level	4
In-Core LOCA • Two simulations at different reactor power levels • Covers small LOCA cases	Moderator High Level PRZ Low Level	2
Boiler feedline pressure trip event(s)	Boiler F/L Low Pressure	1
Main steam line break	Boiler Low Level	1

Table 1: Typical Plant Events Modeled for Reliability Testing

4.3 Modifications to CATHENA Configuration Files

Once the analysis events have been selected, the CATHENA configuration files are modified and run with CATHENA to produce the plant response output files, which will form the basis for reliability test profile development.

The CATHENA user interface is based mainly on data files. The plant thermodynamic model, the initial operating conditions, the event type and the output file specifications are all defined in input data files. The data files are in text format, and can therefore be reviewed and controlled using readily available editors and configuration management tools.

The objective of the CATHENA-based approach is to produce reliability test profiles that reflect the plant responses to analysis basis events. Changes to the thermodynamic and event modeling files are therefore minimal. The most significant changes are to the CATHENA output specification files, which identify the parameters to be logged by CATHENA during the analysis run. The output specification files are revised to output the plant parameters that the trip computers monitor (i.e. the inputs to the trip computer).

4.4 Generation of Baseline Profiles

Once CATHENA simulation has been run for the selected analysis events, the resulting CATHENA output files are converted into the baseline profiles from which the test profiles are built.

Table 1 lists the plant events whose CATHENA models, initially prepared for safety analysis, are reconfigured for test profile generation. Modification and execution of the CATHENA runs will yield approximately fifteen sets of output files, each one modeling a distinct plant event. Together these scenarios exercise every trip parameter.

The first step in converting the CATHENA output files into baseline profiles is to confirm that every trip parameter is exercised, and that the trip signal terminates at a value sufficiently far beyond the setpoint to prevent chattering of the trip computer output. The signal may be manually extrapolated along the trajectory dictated by the simulation if necessary to ensure that the final signal value demands a trip response. The relatively small number of CATHENA output runs means that a manual review of the starting basis is practical.

The second step is to convert the modeled plant parameters into trip computer input signals. For example, the trip computer software in the current design automatically adds a downcomer correction factor to the boiler level signals, therefore the downcomer value used by CATHENA must be subtracted from the boiler level signals before they are transmitted to the trip computer. The parameter ultimately used for the trip decision must correspond to the parameter modeled in the analysis as seen by the trip computer.

The third step is to ensure that every instrument loop providing a trip input signal to the computer is exercised. Many events are analysed for one loop, and the overall plant analysis assumes a symmetrical response on the others. For example, a CATHENA model prepared for a pipe break on reactor outlet header #1 (ROH1) may be credited as representing a similar break on the other three outlet headers (ROH3, ROH5 and ROH7).

Software testing demands explicit tests of individual loop signals, a requirement that is met by expanding one CATHENA output file into baseline profiles by reassigning the value of the input signal demanding a trip to each loop in turn of a multi-loop parameter. In the above example, the CATHENA run resulting in a ROH1 low pressure condition would form one baseline profile, and three more profiles would be obtained by swapping the ROH1 pressure signals with the pressure signal for ROH3, ROH5 and ROH7. Manual review would ensure that related signals, such as PHT flow were similarly swapped as required to preserve the internal consistency of the baseline profile.

It is estimated that the CATHENA output files resulting from the analysis of the fifteen plant events listed in Table 1 will expand into fifty baseline profiles, each of which is a noiseless set of time-dependant trip computer input signals corresponding to a different simulated plant event and known to exercise at least one computer-based trip.

4.5 Expansion of Baseline Profiles to Test Profiles

An automated software tool is used to generate on average, about two hundred unique test profiles from every baseline profile. Some of the functions are described below.

- Each signal is shifted away from the value in the baseline profile by a randomly-selected offset, which is held constant for the duration of the test profile. The random offset simulates instrument calibration error, and serves to increase the proportion of signal space covered by reliability testing.
- Signals may be randomly selected to fail during a test. Four possible modes are constant or intermittent failures to irrational high or low values. Ensuring that the irrational signal alarm logic is executed increases the number of logical paths which the software must follow.
- Different values of the deshading and derippling gains are randomly selected as each profile is generated, and the raw power signals are altered correspondingly.
- Different and sometimes invalid PHT pump modes are selected.
- Random, normally distributed noise is applied to every value of every process signal.

Addition of random effects therefore converts the set of approximately fifty baseline profiles into ten thousand unique reliability test profiles.

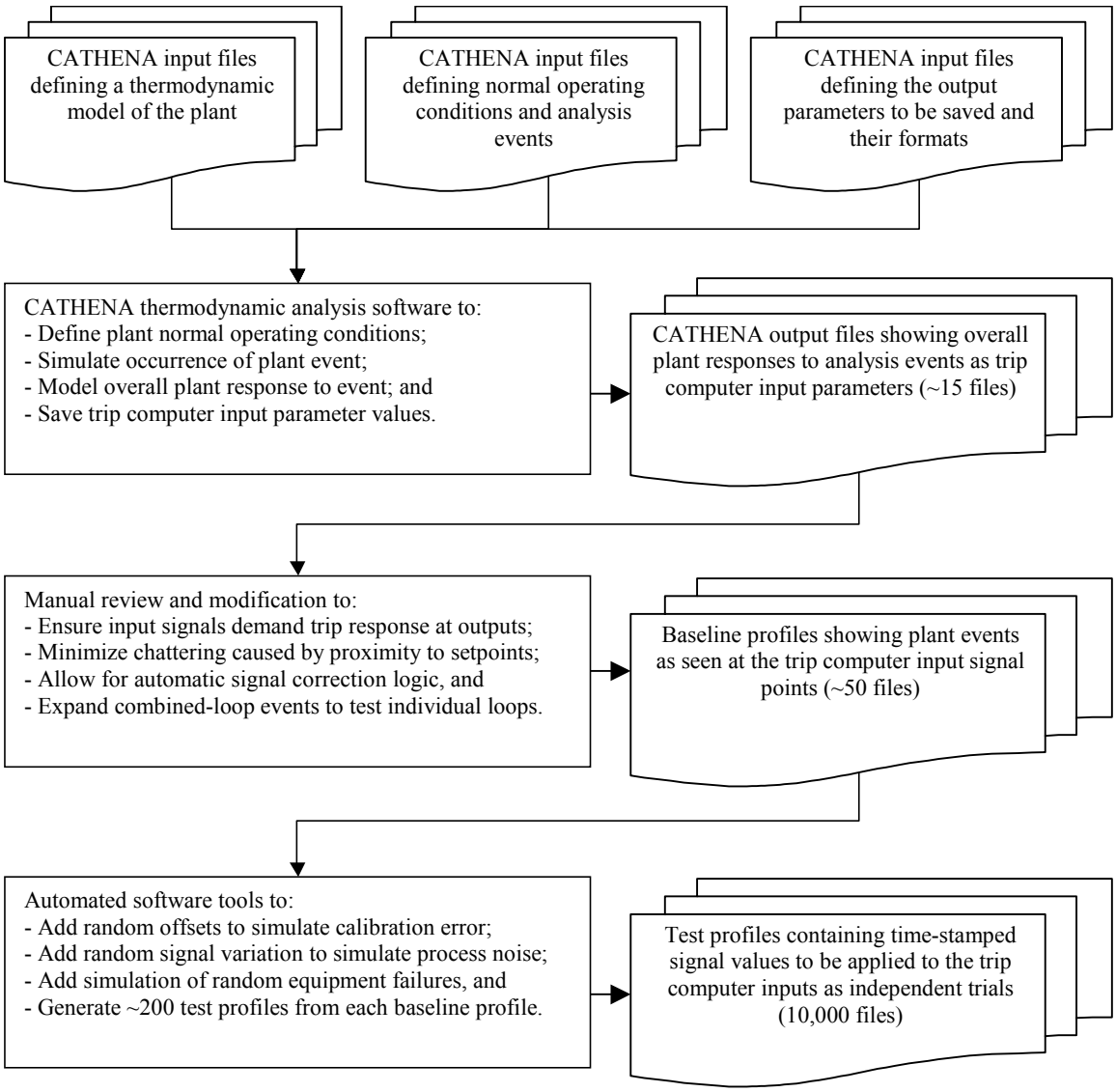

Figure 1: Stages in Test Profile Development

4.6 Independence of Tests

Each test profile is uniquely identified by its baseline profile and the order in which it was generated from the baseline profile. To ensure that the profiles are then run in random order, file names based on the integers from 1 to 10,000 are randomly assigned to each profile. Executing the profiles in numeric order by file name therefore transmits the CATHENA event scenarios to the trip computer inputs in random order.

An initialization profile consisting of a single line of nominal, non-trip signal values is transmitted to the trip computer between test profiles, and the values are maintained until any delayed trips resulting from the previous profile have had sufficient time to clear.

The random sequence of events and the initialization of signals between tests ensure that the requirement for independence trials has been met.

5. Conclusions

The CATHENA-based approach to the development of shutdown system reliability test profiles is a practical means of generating large numbers of realistically modeled, plant dynamic test profiles for reliability testing of shutdown system trip software.

The advantages of the CATHENA-based approach are:

- The latest safety analysis plant model applicable to the current project calculates the critical plant parameter profiles that follow the plant events to which the trip computer is designed to respond;
- The use of existing CATHENA configuration files allows the previous analysis runs to be repeated with only the changes needed to log the trip computer input parameters.
- Manual review of a relatively small number of analysis output files ensures that each baseline profile results in a computer-based parameter trip; and
- Software tools allow limits to be set on the addition of simulated process noise and other random effects to the baseline profiles, thereby meeting both the need for ten thousand random trials and the need to avoid chattering on the trip computer outputs.

Transmitting the CATHENA-based reliability test profiles to the trip computer and test oracle in random order and with an initialization phase between each profile ensures independent trials, and ensures that the trip computer software reliability targets have been achieved.

6. References

[1] J.S. Baxter, A.M. McDonald, F.Y. Lam, and N.D. Thai, "Validation and Reliability Testing of Safety-Critical Software for Wolsong NPP Units 2, 3 and 4", *Proceedings of the American Nuclear Society Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies*, 1996, pp. 1019-1024.

[2] B.N. Hanna, "CATHENA: A Thermalhydraulic Code for CANDU Analysis", *Nuclear Engineering and Design*, v. 180 n.2, March 1998, pp. 113-131.