Research Article

A Statistical Methodology for Determination of Safety Systems Actuation Setpoints Based on Extreme Value Statistics

D. R. Novog¹ and P. Sermer²

¹ Department of Engineering Physics, Faculty of Engineering, McMaster University, Hamilton, Ontario L8S4L8, Canada

² Nuclear Safety Solutions Limited, 700 University Avenue, 4th Floor, Toronto, Ontario M5G 1X6, Canada

Correspondence should be addressed to D. R. Novog, novog@mcmaster.ca

Received 10 September 2007; Accepted 11 February 2008

Recommended by Alessandro Petruzzi

This paper provides a novel and robust methodology for determination of nuclear reactor trip setpoints which accounts for uncertainties in input parameters and models, as well as accounting for the variations in operating states that periodically occur. Further it demonstrates that in performing best estimate and uncertainty calculations, it is critical to consider the impact of all fuel channels and instrumentation in the integration of these uncertainties in setpoint determination. This methodology is based on the concept of a true trip setpoint, which is the reactor setpoint that would be required in an ideal situation where all key inputs and plant responses were known, such that during the accident sequence a reactor shutdown will occur which just prevents the acceptance criteria from being exceeded. Since this true value cannot be established, the uncertainties in plant simulations and plant measurements as well as operational variations which lead to time changes in the true value of initial conditions must be considered. This paper presents the general concept used to determine the actuation setpoints considering the uncertainties and changes in initial conditions, and allowing for safety systems instrumentation redundancy. The results demonstrate unique statistical behavior with respect to both fuel and instrumentation uncertainties which has not previously been investigated.

Copyright © 2008 D. R. Novog and P. Sermer. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1. INTRODUCTION

In existing and new nuclear power plants, a variety of special safety systems are employed which will trigger fast reactor shutdown in the event of an accident or undesirable plant condition. These special safety systems utilize multiple and redundant measurements of certain process and neutronic variables, known as trip parameters, which are continuously monitored against predetermined limits. If a measured trip parameter deviates in an unsafe direction in excess of these predetermined limits, known as trip setpoints, the special safety system will initiate a fast reactor shutdown. Nuclear safety analysis is performed to determine the plant response to hypothetical accident scenarios and to assess the effectiveness of the trip parameters and setpoints in achieving the safety goals (i.e., precluding fuel failures or minimizing public dose). Hence, nuclear safety analysis is a critical component in the operation and regulatory licensing of nuclear power plants.

Historically, a set of bounding analysis methodologies and assumptions were used to determine plant response to these events. As a result of these simplifications, it is impossible to determine the exact margins to safety limits. Furthermore, due to scientific discovery issues combined with plant safety margin deterioration due to component aging, these traditional methodologies predict consequences which may prohibit full power operation. In addition to the above, changes in the regulatory framework for operating reactors are also driving changes in the methodology used to demonstrate plant safety [1]. Furthermore, risk-informed decision (RID) making practices and maintenance optimization [2] at each plant rely on accurate quantification of the impact of upgrades/refurbishment on safety margins. The Canadian Nuclear Safety Commission (CNSC) and the USNRC have recognized that best-estimate predictions of plant response, along with accurate assessments of uncertainties, are an acceptable alternative to more limiting and bounding analyses for demonstrating safety system response [3, 4].

The Canadian CANDU industry is currently pursuing the use of best-estimate and uncertainty (BEAU) methodologies to resolve various issues related to loss-of-power regulation, loss-of-coolant and loss-of-station power accidents [5]. Due to computational limitations, the most recent efforts within the CANDU industry have utilized best-estimate simulations of the limiting fuel channel or detector system within the core. Extensions of best-estimate methodologies to include the effects of the minimization and maximization over the entire core of fuel channels in a CANDU have been performed by Sermer et al. [6, 7], to examine the uncertainty in predicting the maximum fuel-channel power, and by Pandey [8], pressure tube integrity issues. Furthermore, the applications of extreme-value theory are also important in the finance and insurance industries [9] as it can provide estimates of both the likelihood and confidence of rarely occurring events.

The use of extreme-value statistics provides a more accurate framework for establishing the uncertainty in the estimated outcomes by examining not just the uncertainty in individual fuel channels or trip instrumentation responses, but rather the uncertainty in computing maxima and minima of the quantity in question. This paper presents a methodology for determining the required trip setpoints during transient accident analyses of special safety systems using the so-called extreme-value statistics and accounting for the multiple and redundant measurements available within each safety system.

2. BACKGROUND

For a typical CANDU reactor, there are 480 fuel channel assemblies in the reactor core which are fed by two separate figure-of-eight heat transport system loops. Each figure-of-eight loop has 2 heat transport system pumps and 2 steam generators for heat removal and provides coolant flow to half of the fuel channels. The 480 fuel channels contain from 12 to 13 natural uranium fuel bundles at power levels up to approximately 6 mW per channel. A heavy water moderator surrounds each fuel channel assembly and is contained in a calandria vessel. Reactor power is controlled through the reactor regulating system (RRS) which manages bulk and local power levels, as well as monitoring of the core for abnormal occurrences. In the event of abnormal operating occurrences or accidents, regulatory requirements are placed such that fuel and pressure tube failures are precluded. Defense-in-depth was typically employed such that there is a large margin to fuel and pressure tube failure at the time of safety system actuation.

CANDU reactor designs operate at much lower heat fluxes than light water reactor (LWR) designs, and hence the use of dryout (or in the LWR case, departure from nucleate boiling) as an acceptance criteria is excessively conservative since the sheath and fuel temperature excursions in the postdryout regime are much more benign than that under similar LWR conditions. Therefore, for actual CANDU applications, it has been recommended that alternative thermalhydraulic criteria, such as prevention of sheath temperatures exceeding 600°C, be adopted. However to simplify this

methodology, and for consistency to common LWR acceptance criteria, the acceptance criteria adopted in this paper will be the prevention of dryout in all fuel channels

CANDU reactors are equipped with two independent shutdown systems, each with the capability of rendering the core subcritical and each with its own unique set of instrumentation. The instrumentation systems within each shutdown system are divided into three logic channels and within each logic channel there are several redundant instruments measuring plant variables. The shutoff mechanism relays are actuated when trip signals from two-out-of-three exceed their trip setpoint. In the event of an accident at a CANDU station, the transients may be terminated by the RRS monitoring systems or either of the special safety shutdown systems.

Nuclear safety analyses are performed for selected accident scenarios to determine both the setpoints required for shutdown system instrumentation and accident consequences. Computer codes are used to model reactor core physics and heat transport system behavior during postulated transients; and the code predictions are used to establish the trip setpoints required to prevent undesirable consequences. The original nuclear safety analysis for CANDU stations was performed using deterministic assumptions such that the consequences demonstrated in the analysis bounded all possible outcomes for that accident scenario and to provide the most conservative estimate of the required actuation setpoints for the special safety systems. In order to better estimate the actual margins, to provide input for risk-informed decision making, and to better focus plant upgrade activities, best-estimate safety analyses are being proposed as part of the continuous nuclear safety analysis update program. With the advent of statistical methodologies, the focus has now shifted to providing shutdown system trip setpoints with very high probability, or alternatively assessing the probability of failure with existing setpoints. This paper presents the framework for this methodology and demonstrates the application to a simplified bulk power excursion event.

3. METHODOLOGY

3.1. Required trip setpoint

The methodology proposed in this paper provides a statistical treatment of the available instrumentation response as well as the fuel-cooling response which may be applied to best-estimate analyses. Consider a certain accident scenario in a nuclear power plant at a fixed instant in time. For this scenario, there is some value of the shutdown system activation trip setpoint, tsp , which will initiate shutdown such that the safety objectives are met. The value of this trip setpoint could be determined if

- (i) the initial operating conditions at that instant were known exactly,
- (ii) the simulation of the plant response was without error, and if
- (iii) the actual safety system measurements were perfect.

Given the above, a setpoint for each shutdown parameter could then be determined based upon the value of the key instrumented physical at their specified locations in the reactor. This true trip setpoint would provide 100% probability that the safety objective would be met if an accident occurred at that instant in time. In reality, the true setpoints cannot be known due to uncertainty in the models used to predict the outcome and uncertainty in the initial conditions at that instant in time. Even if the true trip setpoint could be established at a given instant in time, the acceptance criterion may still be violated due to uncertainty associated with each instrument used in the special safety systems. Finally, since there are variations in the actual plant conditions caused by fuel burn-up, process system variability, and plant-component aging, these must also be considered in setpoint determination.

What is needed is a required trip setpoint (RTSP) which will cause a reactor shutdown such that there is high probability that the acceptance criteria will be met at a certain reactor configuration, m . The RTSP should account for: (i) the uncertainty in instantaneous plant boundary conditions, (ii) the uncertainty in simulation models and computer codes used to predict the plant response, (iii) the measurement uncertainties related to shutdown system instrumentation, and (iv) the instrument time delays and uncertainties in time delay if necessary. (It is assumed that the instrument response and reactor shutdown on a trip signal are prompt with respect to any true value change. These assumptions are not necessary for this methodology, but are made to simplify the following calculations. Modified derivations are available to account for instrument and shutdown response characteristics.) Once the RTSP for state m is established, a large number of reactor states could be examined and an appropriate statistical lower bound could be determined based on the RTSP for each $m + 1$ considered. The application of the methodology for time-dependent reactor states is discussed in the subsequent sections.

The true trip setpoint for an instantaneous reactor state, tsp_m , is defined as the setpoint required to meet the acceptance criterion given complete knowledge of the initial plant conditions at that instant, perfect computational models for that accident sequence, and perfect measurements. Since these conditions, models, and measurements are not perfect, only an estimate of the setpoint, TSP_m is available. The relationship between this estimate and true value is given as

$$\text{TSP}_m = \text{tsp}_m(1 + \varepsilon_m), \quad (1)$$

where ε_m is the error in the estimated setpoint at that instant in time and is a random variable which considers errors in the initial conditions, plant response models and instrumentation uncertainty and consequently TSP_m is a random variable. What is needed is the required trip setpoint based on the random TSP_m , which will have a high probability of

$$\text{RTSP}_n \begin{cases} \leq \text{tsp}_m & \text{high going limit,} \\ \geq \text{tsp}_m & \text{low going limit.} \end{cases} \quad (2)$$

For simplicity, the remainder of this section will deal with the trip setpoint at a given instant in time and hence the subscript, m , is dropped. For the sake of convenience, the foregoing paper will examine high-going trip setpoint limits (i.e., a variable that will trip the reactor if it exceeds some maximum value). The application of the methodology for time-dependent reactor states is discussed in the subsequent sections; and for low-going trip setpoints, the methodology is a simple extension.

3.2. Acceptance criteria

As discussed in Section 2, dryout must be prevented in each of the 480 fuel channels such that

$$\min_{i=1,480} (\text{mtd}_i) > 1.0 \quad (3)$$

which specifies that the minimum margin to dryout (mmtd) over the entire CANDU core must be greater than unity. (For LWRs an alternative such as $(\text{mtd} + \gamma)$ may be used, where γ is a predefined margin to the departure from nucleate boiling.)

Specifically, mtd_i is the true value of the margin to dryout in channel i computed from

$$\text{mmtd} = \min_{i=1,480} [\text{mtd}_i] = \min_{i=1,480} \left[\frac{\text{ccp}_i}{\text{cp}_i} \right], \quad (4)$$

where cp_i is the instantaneous channel power in channel i and ccp_i is defined as the critical channel power in channel i . The critical channel power (CCP) corresponds to the channel power that would be required to initiate dryout for the same thermalhydraulic inlet boundary conditions. During the progression of the accident, the margin to dryout will be a function of time t , and hence it is required that the minimum margin to dryout, mmtd, is

$$\text{mmtd} > 1.0 \quad (5)$$

for all times of interest. Equation (5) can be reformatted using order statistics as

$$\text{mmtd} = \text{mtd}_{(1)} > 1.0, \quad (6)$$

where the subscript (5) indicates the smallest value in the ordered set mtd.

3.3. Safety system actuation

Safety and shutdown systems in a CANDU plant are actuated when the multiple and redundant special safety system instruments exceeds the trip setpoint for that variable. For the following analysis, the instrumentation response is measured as a fractional value of the trip setpoint and denoted as f_j , where j is the instrument number. Furthermore, the analysis will consider one shutdown system with instruments grouped into one of the three logic channels labeled D, E, and F. Within each logic channel, instrumentation measures the plant response and compares the measured value to the predetermined trip setpoint; and if it exceeds this threshold,

a trip will register on that logic channel. As mentioned, if two-out-of-three logic channels register a trip, the safety system will activate.

At the point in the accident transient where the margin to dryout approaches unity, the setpoint is selected such that at least one of the following holds:

$$\begin{aligned} & \frac{1.0}{\min(\max[f_j^D], \max[f_j^E])} < 1.0, \\ \text{or } & \frac{1.0}{\min(\max[f_j^D], \max[f_j^F])} < 1.0, \\ \text{or } & \frac{1.0}{\min(\max[f_j^E], \max[f_j^F])} < 1.0, \end{aligned} \quad (7)$$

where D, E, and F are the labels for each of the logic channels in a safety system. The above expression ensures that in the event the margin to dryout decreases to its acceptance criteria, then the trip will actuate the shutdown system based upon 2-out-of-3 logic channels exceeding the setpoint. For comparison to order statistic approaches, the trip signals can be grouped into a single set, s , and the appropriate order statistic selected. Therefore, s is given as

$$s = [f_{(n)}^D, f_{(n)}^E, f_{(n)}^F], \quad (8)$$

where the subscript (n) denotes the highest detector reading in each ordered set of responses within that logic channel. For example, for the 2-out-of-3 logic trip,

$$\text{mtt} = s_{(2)} < 1.0, \quad (9)$$

where mtt is the margin to trip and $s_{(2)}$ denotes the second smallest value in the ordered set s . It should be noted that in many licensing applications, the goal is to demonstrate a reactor trip in the analysis on 3-out-of-3 logic channels, in which case the minimum margin to trip, mmtt, is

$$\text{mmtt} = s_{(1)} < 1.0. \quad (10)$$

It can be shown that for the more general case for k -out-of- n trip logic, the proper order statistic for the margin to trip is

$$\text{mmtt} = s_{(n-k+1)} < 1.0. \quad (11)$$

Hence the true trip setpoint can be selected for a given accident such that (10) holds at the point in the transient where the margin to dryout approaches unity.

3.4. Margin to dryout uncertainty

The methodology used to select the setpoint above is applicable to only situations where perfect information is available (i.e., where the true values can be established). In reality each of the variables discussed above is subjected to both measurement and simulation uncertainties which may have components that are a function of space and time. For example, instruments in different parts of the core may have differing uncertainties, the simulated transient code predictions at the measurement locations may be delayed/accelerated in time,

and the critical channel power in any of the 480 channels may be over or under predicted at any instant. In addition, there may be a noise component in the actual instrument behavior.

First, consider three hypothetical CANDU reactor cores with 1 fuel channel, 5 identical fuel channels, and 10 identical fuel channels, respectively; and assume initially that there is an independent random uncertainty in the margin to dryout prediction in each channel such that

$$\text{MTD}_i = \text{mtd}_i(1 + \epsilon_i^{\text{mtd}}), \quad (12)$$

where ϵ_i^{mtd} denotes the error in channel i . For demonstration purposes, it will also be assumed that the errors are normally distributed, independent, with mean 0.0, and standard deviation of 4.0% (i.e., a typical value of CCP uncertainty in CANDU applications) and that the true value are equal. The estimate of the minimum margin to dryout will therefore be

$$\text{MMTD} = \min_{i=1,z} [\text{mtd}_i(1 + \epsilon_i^{\text{mtd}})], \quad (13)$$

where z is the number of channels in the hypothetical reactor being considered. At a given point in an event sequence assume that the true minimum margin to dryout decreases to a value of 1.08. Monte-Carlo simulation can be performed to determine the probability of predicting a trip

$$P\{\text{MMTD} \leq 1.0\}. \quad (14)$$

For the cases being considered, the probabilities are 3.2%, 9.8%, and 27.8% for the 1, 3, and 10 fuel channel reactor configurations, respectively, (the results for this simplified case of equal true values are comparable to the results obtained using the usual order statistics). This is a critical finding because it indicates that as the number of channels being simulated is increased, there is an increasing probability of declaring a false-positive when testing for fuel channel dryout (i.e., there is a 27.8% probability for a predicted value to indicate dryout when in fact the true margins were 1.08). This is to be expected because the mean of an extreme value distribution shifts in the direction of the extreme function. If at a certain point later in the transient the true margin to dryout in each channel becomes 1.01, then the probability of the estimates predicting dryout are 40.1%, 78.7%, and 99.4% for hypothetical cores containing 1, 3, and 10 fuel channels, respectively. For this simplified demonstration, it has been shown that increasing the number of fuel channels considered within the minimization process tends to increase the probability of estimating that dryout has occurred.

As an extension to this demonstration, consider the same transient but for a case where the true minimum margin to dryout has reached unity. At this point in the transient, the probability of demonstrating a trip is 50.0%, 87.6%, and 99.9%, respectively, or alternatively, there is a 50.0%, 12.4%, and 0.1% probability that dryout will not be predicted when in fact the true margin to dryout has reached 1.0 (i.e., a Type 1 error). It is clear that in considering the random nature of the several channel responses, the probability of Type 1 errors is reduced.

As an extension to the hypothetical reactor cases studies above, assume that the true values for each of the fuel

TABLE 1: Influence of the number of participating fuel channels in the probability of missing dryout.

q [fraction]	Number of fuel channels	Probability of predicting dryout [%]	Probability of Type 1 error [%]
1.08	1	4.7	0.0
	2	9.3	0.0
	3	13.7	0.0
	5	21.5	0.0
	10	38.4	0.0
1.04	1	19.3	1.1
	2	35.8	2.0
	3	47.8	2.1
	5	66.4	2.4
	10	88.6	1.5
1.02	1	34.0	7.0
	2	55.4	8.1
	3	70.6	8.1
	5	86.2	5.2
	10	98.3	1.1
1.00	1	50.3	18.7
	2	75.4	14.3
	3	88.2	9.1
	5	96.9	2.6
	10	99.9	0.1

channels are not equal. For this demonstration, a set of random true values is selected for each channel based on a normal probability distribution of $\pm 2\%$ (typical scatter in margin to dryout in a CANDU reactor for the high-power channel) centered about a mean value of q . For this set of true values, Monte-Carlo simulations were performed with random, normal, and independent uncertainties assigned to each channel. The probability of predicting dryout was recorded along with the probability of a Type 1 error given as

$$P\{\text{MMTD} > 1.0 \mid \text{mmt} \leq 1.0\}. \quad (15)$$

The process of generating an initial set of true margins, then performing Monte-Carlo simulations about these values, was repeated a large number of times to determine the average probability of predicting dryout along with the average probability of creating a Type 1 error (the total number of simulations exceeded 10^6). The results of this study with no additional allowances are shown in Table 1.

The above example is for the special case where all fuel channels have margin to dryout within 2% and where the uncertainty in estimation is 4%. Table 1 shows that as the mean of the true margin to dryout decreases, the probability of predicting a trip increases for a core with a fixed number of fuel channels. Further, it shows that for a fixed mean true value, the probability of predicting a trip increases with the number of channels. The Table also shows that the probability of a false-negative, that is, predicting no dryout when indeed it

has occurred, behaves nonmonotonically with respect to the number of channels considered or a typical Type 1 statistical error. The fundamental behavior that leads to this nonmonotonic nature has to do with the minimization function being performed. For example, in each permutation of true values for the simplified 2 fuel channel core there is a certain probability that channel A will have to lowest true margin to dryout. However, when the Monte-Carlo uncertainty simulation is performed considering the errors in estimating the margin to dryout, there is a nonzero probability that the predicted value in channel B will be lower than the predicted value of channel A. Therefore, for permutations where the estimate in channel A is in an unsafe direction, there is a probability that the estimate in channel B will be such that it compensates for that error. Note for this situation, the channel with the lowest margin to dryout was incorrectly identified, but the error in channel B assists in reducing the probability of an overall false-negative prediction in the absolute minimum over channel A and B. The larger the number of channels considered, the larger the potential for a prediction to compensate for a nonconservative prediction in channel A.

Figure 1 shows the probability of missing a real occurrence of dryout as a function of the reducing initial true margin to dryout in the channels for results considering 1, 2, 3, 5, and 10 fuel channels. As the value of the mean margin to dryout in the figure decreases, there is an increasing probability that dryout may physically occur in one or more channels. As the margin decreases to 1.0, it is evident from the figure that for estimates involving small numbers of, or single, channels the probability of missing dryout increases significantly. This is contrary to the nonmonotonic nature of the cases involving 5 or more fuel channel estimates, where the probability of missing dryout reaches a maximum and then decreases. For the hypothetical case considered when 10 or more fuel channels have true values within a band of 2%, there is less than a 2% probability of missing over the entire range of possible margins to dryout. This is a significant conclusion as it indicates that the best estimate of the minimum margin to dryout over the 10 channels provides a very accurate indication of actual occurrences of dryout.

Within the CANDU nuclear industry, this type of behavior is commonly termed extreme value statistics (EVS) since the behavior results from maxima and minima functions as applied to the random variables of interest [7]. This has extremely important ramifications in the level of probability assigned to dryout in probabilistic methods, and indicates that traditional best estimate CANDU approaches which utilize best estimate simulations for the limiting channel response are inappropriate. For any best-estimate analysis, all fuel channels, or alternatively the group of channels where the minimum margin to dryout may occur, must be considered in order to capture the true probabilities related to accident consequences. Fuel channels that have a nonzero probability of containing fuel that may undergo dryout are often termed *participants*. This terminology reflects the fact that these specific channels have a reasonable statistical probability of participating in the maximization or minimization functions.

FIGURE 1: Probability of not predicting dryout when dryout has actually occurred for hypothetical cores with 1, 2, 3, 5, and 10 fuel channels.

It is clear that in the application of the parental errors to the margin to dryout, not all components will behave in an independent manner. For example, for fuel channels connected to common reactor inlet headers in a CANDU reactor, a component of the flow, temperature, and pressure uncertainties which lead to CCP uncertainties may be common to all channels in that core pass (i.e., an uncertainty in a header system response based on computer code such as CATHENA or TRACE will cause a common uncertainty in the margin to dryout in all fuel channels connected to that header). Therefore, an error structure is required of nature:

$$MTD_i = mtd_i(1 + \varepsilon_i^{mtd})(1 + \varepsilon_{common}^{mtd}), \quad (16)$$

where ε_{common} represents a common error associated with a group of channels in the core; and ε_i is the channel specific component of the error.

3.5. Instrumentation response uncertainty

For the special safety system, instruments estimates of the results will deviate from the true values due to

- (i) computer code simulation uncertainties, and
- (ii) errors in the simulation of the time response characteristics of the measurement device.

Hence for each instrument, the simulated response, F_j , will be

$$F_j = f_j(1 + \varepsilon_j^f), \quad (17)$$

where ε_j^f is the error in simulation of the instrument response. For a high going limit, the instrument with the largest response in each logic channel will initiate a trip of that channel. Therefore, for a 3-out-of-3 trip requirement, the estimated minimum margin to trip at each instant in the transient is given as

$$MMTT = \frac{1.0}{S_{(1)}}, \quad (18)$$

where S is defined as

$$S = [F_{(n)}^D, F_{(n)}^E, F_{(n)}^F], \quad (19)$$

and (n) denotes the highest reading in each ordered set of F . Alternatively, the minimum margin to trip error can be defined using

$$MMTT = mtt(1 + \varepsilon^{mmtt}), \quad (20)$$

where ε^{mmtt} is the error in the minimum margin to trip and is a complex function of the number of instruments in each logic channel and the simulation uncertainty in each instrument.

Similar to the exercise performed on the margin to dryout, an exercise is provided to illustrate these concepts for the margin to trip variable. For this demonstration, various amounts of instrument redundancy in each logic channel are considered (from one instrument per channel up to 4 responding instruments per channel) and 3-out-of-3 trip logic is assumed. A set of true values is randomly generated for each instrument about a mean value as shown in Table 2 and with a standard deviation of 3%. For a given set of true values, a Monte-Carlo analysis is performed by applying a random, normal, and independent uncertainty with standard deviation of 3% to each detector and then computing the simulated minimum margin to trip as shown in (22). The probability of simulating a safe margin to dryout for cases where the true margin falls below unity is then determined from

$$P\{MMTD > 1.0 \mid mmtt \leq 1.0\}. \quad (21)$$

This entire process is then repeated a large number of times for a new set of randomly selected true instrument responses and an average is then determined. The results of this exercise are shown in Table 2.

Based on these results, the probability of predicting a trip increases with the number of detectors as expected since there is a larger probability that at least one instrument will read sufficiently high to actuate the logic channel for any random perturbations. The probability of predicting a reactor trip increases as the mean of the true instrument response approaches the trip setpoint as expected. This is expected as the maximization will tend to increase the predicted value within each logic channel. Examining the Type 1 error results shows nonmonotonic behavior which is dependent on the proximity of the true instrument responses to the trip setpoint and the number of instruments within each logic channel. This Table shows a fundamental difference in the

TABLE 2: Influence of the number of available detectors on the probability of missing a required trip.

Mean true detector reading	Instruments per Logic channel	Probability of trip [%]	Probability of Type 1 error [%]
0.90	1	0.0	0.0
	2	0.0	0.0
	4	0.0	0.0
0.95	1	0.1	0.2
	2	1.0	0.9
	4	4.7	2.0
0.98	1	2.8	4.4
	2	15.2	12.9
	4	45.4	17.7
0.99	1	6.2	10.3
	2	27.2	23.2
	4	66.7	18.3
1.00	1	12.4	20.0
	2	42.2	25.6
	4	83.0	12.4

behavior of the trip instrumentation system as compared to the fuel channel dryout cases described previously. Although increasing the number of instruments may improve the availability of the logic system for the purposes of reliability assessments, it has a negative effect in terms of the trip predictive capability. Specifically, if a single instrument is overpredicted within the logic channel, it will cause the logic channel to trip erroneously; and, hence, the more instruments within each of the logic channels, the more probable that a single prediction will occur which trips that logic channel; when in fact the true values would indicate otherwise. Therefore, it is crucial for safety analysis predictions to include not just a single *worst responding* instrument in each channel, but rather the entire system must be simulated and the appropriate allowance or factor of safety applied.

3.6. Setpoint confidence level

Most statistical definitions for statistical setpoint and setpoint analyses, such as ISA 67.04 and CNSC regulatory guide G-144, require trip setpoints and instrumentation to provide a 95% probability with 95% confidence, or the so-called 95/95 approach. Within the context of the ISA guide [10, 11], the definition utilized for this paper is as follows:

The setpoint must provide at least a 95% probability of reactor shutdown system initiation before the acceptance criterion is exceeded with at least a 95th percentile confidence bound on the plausible reactor operating states where the setpoint need be effective.

Within the context of CANDU reactor operations, the processes show some variability such that the initial core configuration prior to an accident may take on a variety of values. Therefore, within setpoint analyses, it must be demonstrated that there is at least a 95% probability of trip over

95% of the available operating states. Practically, this can be achieved by performing uncertainty analyses about each initial reactor configurations and determining a trip setpoint that provides 95% probability of trip before the acceptance criteria, and then repeating this analysis over a large number of possible core configurations. The 95th percentile lower confidence bound over these setpoints provides will meet the 95/95 criteria specified above.

The preceding sections have examined the margin to dryout and margin to trip behavior in isolation. The following sections will integrate these results into a more realistic trip setpoint demonstration.

4. TRIP SETPOINT CALCUALTION

4.1. Trip setpoint formulation

From a given reactor initial state, it must be shown that during an accident, the margin to trip is less than one at the instant that the margin to dryout reaches unity. If the true value of all quantities were known then the trip setpoint selected would be equal to the instrument reading at the time when the true margin to dryout reached unity. The setpoint can be defined by examining an accident transient from time zero and determining the trip setpoint from the following condition:

$$\text{if (mmtd} \leq 1.0) \text{ then } (\text{tsp} = s_{(k-n+1)}) \quad (22)$$

for k -out-of- n trip logic. However, due to uncertainties in the minimum margin to dryout and minimum margin to trip, detailed statistical analyses are required to assure that the required trip setpoint will actuate the reactor prior to dryout with high probability. Since the true values for each quantity above cannot be established, only the estimated trip setpoint, TSP, can be established:

$$\text{if (MMTD} \leq 1.0) \text{ then } (\text{TSP} = S_{(k-n+1)}). \quad (23)$$

As stated previously, the error in this estimated trip setpoint can be established as

$$\varepsilon = \frac{\text{TSP} - \text{tsp}}{\text{tsp}}, \quad (24)$$

where ε is the error in the estimated trip setpoint. It should be noted that the error in the trip setpoint cannot be evaluated directly since it requires knowledge of the true trip setpoint. To estimate this distribution the statistical surrogate principle, or similar bootstrap method, must be employed [12]. Finally, what is required in practice is a suitable factor, η_α , which can be applied to any estimate of the trip setpoint such that the required trip setpoint meets the established probability and confidence limits for the safety acceptance criterion, that is,

$$\text{RTSP} = \text{TSP}(1 - \eta_\alpha), \quad (25)$$

where TSP is an estimate of the trip setpoint and RTSP is the required trip setpoint to ensure the safety acceptance criterion, are established to the mandated probability and confidence level. As mentioned in Section 3.6, this is determined

by computing the 95th percentile error in the setpoint estimates for a large number of operating states, and taking the lower bound 95th percentile confidence level over these potential operating configurations.

4.2. Numerical demonstration

As an illustration of the setpoint methodology, consider a hypothetical bulk power excursion accident in a CANDU reactor where the true power is increasing exponentially with time constant 60 seconds and with a typical initial margin to dryout of 1.40. The assumed quantities for this case are as follows.

- (i) In a given CANDU reactor, there are approximately from 10 to 20 fuel channels with very comparable margins to dryout, so that for this example 10 fuel channels are included with random initial margins to dryout characterized by a uniform distribution with mean $1.40 \pm 3\%$.
- (ii) There are typically at least 3 neutronic detectors in each logic channel which will respond to a power event so that 3 are included in this exercise along with initial detector reading with a scatter represented by a uniform distribution with $\pm 2.5\%$. Since the neutrons detectors in a CANDU are normalized to 100% FP readings and are calibrated within this band regularly, the assumed true initial detector readings have a mean of 1.0 with a uniform scatter of $\pm 2.5\%$.

Similar to the procedure in previous sections, the hypothetical true values were first randomly selected for the 10 fuel channels and the 3 detectors in each logic channel, with each of these randomizations corresponding to different possible initial reactor configurations. Then the transient was superimposed on these readings such that for this hypothetical reactor core both the true margin to dryout and true detector responses were known. Based on these transient responses, the true value of the setpoint, tsp_m , could be determined using (22). This process was then repeated by generating a new set of initial margins to dryout and trip for the channels and detectors in the core and the true trip setpoint for each core state was logged.

Monte-Carlo uncertainty calculations were then performed about each of 5000 core state utilizing the following uncertainties in key parameters:

- (i) a fuel channel independent uncertainty in estimating the margin to dryout was applied to each fuel channel which was characterized by a normal distribution with standard deviation of 4%,
- (ii) a random uncertainty in determining the initial margin to dryout that is common to all fuel channels and characterized by a normal distribution with standard deviation of 1% was applied. These types of uncertainties may arise from uncertainties related to common input (e.g., header inlet temperature uncertainties in a CANDU design),
- (iii) a random, and detector independent uncertainty in determining the initial detector readings, character-

FIGURE 2: Trip setpoint error distribution for a selected core state.

ized by a normal distribution with a standard deviation of 2%, was applied. This may be caused by uncertainties in the local reactivity during the transient or in modeling of each unique detectors neutron flux.

- (iv) an uncertainty in the instantaneous power which commonly affects the margin to trip and detector readings was implemented by applying a normal distribution with standard deviation of 0.5%. This type of uncertainty is commonly associated with uncertainties related to total reactor power and/or reactivity insertion.

In order to demonstrate the statistical methodology, the Monte-Carlo procedure was implemented as follows:

- (i) an initial core state, m , was selected from the 5000 cases and the transient power applied to each variable. For the selected core state, the true value of the trip setpoint was determined using (22).
- (ii) for the selected core state a set of estimated variables, m , is generated for each channel and detector using the uncertainty distributions outlined above. The transient power was then applied to these values along with the uncertainty in instantaneous power by using discretized time steps on the order of 0.05 second.
- (iii) based on the transient behavior of the estimated variables, an estimated setpoint was determined using (23).
- (iv) an error was then calculated as the difference between the estimated and true setpoints using (24).
- (v) many sets of estimated variables, n , are generated (i.e., more than 1×10^5) for the hypothetical set of true values, m . The setpoints are determined and a distribution of possible errors is produced. From this distribution, the 95th percentile bounding error value can be determined. Figure 2 shows a sample of the error distribution about a selected operating state. The 95th percentile probability of the error, ε_{95} , for this initial core state was -0.004% .

- (vi) a new core state is then selected, $m+1$, (i.e., a new set of true values) and the procedure outlined in steps from (ii) to (v) is repeated, and the 95th percentile error, ϵ_{95} , is recorded for each iteration.
- (vii) A probability distribution of all ϵ_{95} is shown in Figure 3 based on the results of approximately 5×10^8 simulations (i.e., $m \times n$), and from this distribution an upper confidence limit on the error over all reactor states, η_{95} , is selected.

Figure 3 shows the distribution of 95th percentile errors determined based on Monte-Carlo analyses about each of the 5000 cases (i.e., based on the error determined for each of the 5000 initial core states with 1.0×10^4 Monte-Carlo passes for each state, or more than 10^7 simulations). It should be noted that the distribution is much tighter than the individual error distributions about any given single initial core state and follow a general Gumbel-type of distribution associated with extreme value statistics. The 95th percentile upper confidence limit over all 5000 operating states considered is 1.2%, or alternatively for a 95/95 required trip setpoint the best estimate for a given reactor configuration would need to be reduced by 1.2%.

This 95th percentile confidence limit over all of the 95% probabilities for each core state provides a 95/95 probability and confidence statement which is consistent with that defined in ISA 67.04 for safety instrumentation requirements. Finally, the value of η_{95} can be used to determine the required trip setpoint based on an estimated trip setpoint using

$$\text{RTSP} = \text{TSP}(1 - \eta_{95}). \quad (26)$$

Equation (26) utilizes the statistic η_{95} to modify the best estimate trip setpoint, TSP, such that RTSP will provide a trip prior to dryout with high confidence. Note that depending on the number of fuel channels and the scatter in their margin to dryout, the statistic η_{95} may be either positive or negative. A positive value indicates the setpoints determined using best-estimate simulation should be decreased by an appropriate amount to obtain a 95/95 result, while a negative value indicates that the best-estimate simulations are likely to under predict the true required setpoint due to the tendency of the minimum margin to trip to be underestimated (i.e., due to participants).

4.3. Sensitivity to power transients

Figure 4 shows the trend in η_{α} as a function of the number of fuel channels considered in the demonstration. This is equivalent to considering situations where the core has less participants (i.e., core configurations that have outliers with margins to dryout substantive less than the surrounding fuel channels). This figure shows that for core states where outliers are a concern the compliance allowance factor increases. This is expected since the participation effect is reduced, and there is a smaller probability that other fuel channels may compensate for errors in the estimates of an outlier. (An alternative method for examining the effects of outliers would be to increase the distribution in the true channel powers and assess the impact on the uncertainty allowance.)

FIGURE 3: Distribution of 95th percentile trip setpoint errors over all core states.

FIGURE 4: Allowance factor as a function of fuel channels and the transient accident speed.

The effect of different exponential power transients is also shown in Figure 4 for exponential time constants of 1 second, 10 seconds, 60 seconds, and 120 seconds as a function of the number of fuel channels participating. The results show that the allowance factor becomes negative as the number of participating channels increases towards 20 (i.e., the best-estimate simulations themselves will provide at least a 95% probability and level of confidence). Furthermore, Figure 5 shows the behavior of the allowance factor for increasing numbers of participating detectors and for various power transient time constants. From Figures 4 and 5 it can be concluded that the allowance factor is not sensitive to the transient power rate (The changes in the allowance factor are

FIGURE 5: Allowance factor behavior as a function of the number of detectors in each logic channel and as a function of transient speed.

within the numerical accuracy of the Monte-Carlo simulations). It is an encouraging result of this methodology that the allowance factor is not significantly affected by the speed of the transient being considered, at least for the stylized LOR considered in this work.

5. CONCLUSIONS

A methodology for computing 95/95 trip setpoints for transient nuclear safety analysis has been presented which utilizes estimates over all fuel channels and detectors in a reactor core, and hence the errors in the maxima and minima predictions can be estimated. These estimates are used to ensure that there is a high probability and confidence that the acceptance criteria will be met for an accident. The methodology developed above represents a unique application of uncertainty analysis for estimation of setpoint errors required for safety analysis.

The statistical properties of the margin to dryout and margin to trip are separately investigated and in particular the behavior of the minimum estimated margin to trip and minimum margin to dryout are discussed. In general, it was observed that the number of fuel channels and detectors simulated impact the error observed in estimating the maxima or minima. These concepts were then applied to a hypothetical reactor transient involving a bulk power excursion event. Based on these simulations, the statistic used to correct the best estimates in trip setpoint was determined based upon the methodology outlined in this paper. For the hypothetical accident, the statistic decreases with increasing number of fuel channels and decreasing number of detectors. Furthermore, it has been demonstrated that the allowance factor increases only slightly with faster transients.

Finally, it is strongly recommended that for any best-estimate analysis, all fuel channels and detectors are appropriately modeled, or alternatively a group of channels where the minimum margin to dryout may occur and most probable tripping detectors must be considered in order to capture the true probabilities related to accident consequences. Furthermore, while this paper examined the margin to dryout behavior for a CANDU pressurized heavy water reactor, the results may be adopted for LWR analyses provided that the required margin to DNB is used.

ACKNOWLEDGMENTS

The authors would like to thank the University Network of Excellence in Nuclear Engineering (UNENE), the Natural Sciences and Engineering Research Council of Canada (NSERC), and Nuclear Safety Solutions (NSS) for their support of this work.

REFERENCES

- [1] Canadian Nuclear Safety Commission, Proposed Regulatory Standard-S310, 2006.
- [2] G. Geisler, S. Hellweg, and K. Hungerbühler, "Uncertainty analysis in life cycle assessment (LCA): case study on plant-protection products and implications for decision making," *International Journal of Life Cycle Assessment*, vol. 10, no. 3, pp. 184–192, 2005.
- [3] Canadian Nuclear Safety Commission, Regulatory Guide G-144, "Guidelines for establishment of shutdown system trip parameter effectiveness", May 2006.
- [4] Technical Program Group, "Quantifying reactor safety margins: application of CSAU methodology to a LBLOCA," EG&G Idaho, Inc., NUREG/CR-5249, December 1989.
- [5] J. C. Luxat, R. G. Huget, and F. Tran, "Development and application of Ontario power generation's best estimate nuclear safety analysis methodology," in *Proceedings of the International Meeting on Best Estimate Methods in Nuclear Installation Safety Analysis (BE '00)*, Washington, DC, USA, November 2000.
- [6] P. Sermer and C. Olive, "Probabilistic approach to compliance with channel power license limits based on optimal maximum uncertainty," in *Proceedings of the American Nuclear Society Annual Conference*, Philadelphia, Pa, USA, June 1995.
- [7] P. Sermer, G. Balog, D. R. Novog, E. A. Attia, and M. Levine, "Monte Carlo computation of neutron overpower protection trip set-points using extreme value statistics," in *Proceedings of the 24th Annual CNS Conference*, Toronto, Ontario, Canada, June 2003.
- [8] M. D. Pandey, "Extreme quantile estimation using order statistics with minimum cross-entropy principle," *Probabilistic Engineering Mechanics*, vol. 16, no. 1, pp. 31–42, 2001.
- [9] P. Embrechts, C. Klüppelberg, and T. Mikosch, *Modeling Extremal Events for Insurance and Finance*, Springer, Berlin, Germany, 1997.
- [10] ANSI/ISA Standard S67.04-2000, "Setpoints for nuclear safety related instrumentation," February 2000.
- [11] ISA Recommended Practice RP67.04.02-2000, "Methodologies for the determination of setpoints for nuclear safety related instrumentation," January 2000.
- [12] W. H. Press, B. P. Flannery, S. A. Teukolsky, and W. T. Vetterling, *Numerical Recipes*, Cambridge University Press, Cambridge, UK, 1986.