AN INTELLIGENT SAFETY SYSTEM CONCEPT FOR FUTURE CANDU REACTORS

H.W. Hinds*

ABSTRACT

A review of the current Regional Overpower Trip (ROPT) system employed on the Bruce NGS-A reactors confirmed the belief that future reactors should have an improved ROPT system. We are developing such an "intelligent" safety system. It uses more of the available information on reactor status and employs modern computer technology. Fast, triplicated safety computers compute maps of fuel channel power, based on readings from prompt-responding flux detectors. The coefficients for this calculation are downloaded periodically from a fourth supervisor computer. These coefficients are based on a detailed 3-D flux shape derived from physics data and other plant information. A demonstration of one of three safety channels of such a system is planned.

NOMENCLATURE

Symbol	Description	Units
a	coefficients	dim'less
C,C´	flux mapping matrices	
D	diffusion coefficient	m
E,E´	channel power mapping matrices	
f	"deflection", modifying function	dim'less
F	"force"	dim'less
H	flux-to-power conversion factor	$W \cdot n^{-2} \cdot m^2 \cdot s$
P	channel power	W
Q	dynamic error margin function	dim'less
r	distance (normalized)	dim'less
x,y,z	spatial co-ordinates (normalized)	dim'less
Σ	macroscopic cross section	m^{-1}
	Σ_a = absorption	
	Σ_f = fission	
ν	number of neutrons per fission	dim'less
ϕ	flux	$n \cdot m^{-2} \cdot s^{-1}$
ψ	flux distribution from diffusion code	$n \cdot m^{-2} \cdot s^{-1}$

Superscripts

~	measured
^	mapped, estimated using the mapping scheme
¯	average

Subscripts

i	force (or detector) index
j	channel index
k	bundle index
M	using mapping (vanadium) detectors
max	maximum
S	using safety (platinum) detectors

1. INTRODUCTION

1.1 Historical Background

Due to economic incentives, the design fuel ratings of CANDU* reactors have increased over the years. The current limit is based on the rating at which centre-line fuel melting occurs; the consequences of this event are somewhat speculative and considered undesirable. The regional overpower trip (ROPT) systems in Bruce NGS-A and subsequent reactors are designed to prevent fuel melting.

Under CANDU operating conditions, melting can occur only after a breakdown in heat transfer to the two-phase coolant, i.e. after dryout. To compute the thermal power required to melt fuel in a given channel, the following thermohydraulic parameters and correlations are required:

- axial heat flux profile
- dryout correlation (point values)
- coolant flow, inlet temperature, pressure
- post-dryout heat transfer.

Using nominal conditions for the above, the designers of Bruce NGS-A computed the channel power at which centre-line melting occurs and obtained a channel power limit, after applying suitable error margins.

The "measured" maximum channel power in a Bruce reactor is inferred from a set of "readings" from platinum self-powered flux detectors. The relationships between maximum channel powers and detector readings were established during the design studies. The designers chose a large set of flux shapes by considering various combinations of reactivity control device positions; some shapes also included dynamic xenon effects. For each shape, they calculated the detector readings and maximum channel power. The designers then found a set of trip settings which ensured that, for every shape considered, the reactor would trip before the maximum channel power exceeded the pre-determined limit. They performed all the above calculations using an equilibrium-fuelled reactor.

*Atomic Energy of Canada Limited
Research Company
Chalk River Nuclear Laboratories
Chalk River, Ontario
K0J 1J0

*CANada Deuterium Uranium

For actual reactors, having fuels of varying burnups, the operators add a channel power peaking factor (CPPF) to the detector calibrations to account for the channel-to-channel ripple.

This design process yielded a system that was relatively simple to implement: in operation, each detector output is compared to its trip setting* to decide whether to trip or not. Conventional analog/relay hardware is used to execute the trip logic.

There are two ROPT systems at Bruce NGS-A, corresponding to the two shutdown systems, SDS1 and SDS2. Each system is triplicated in the conventional manner to ensure reliability, and each safety channel contains approximately 13 detectors for SDS1 and 6 detectors for SDS2. Future reactors, e.g. Bruce NGS-B will have slightly more detectors per safety channel.

Detector calibration is the main weakness of the Bruce ROPT concept. When the reactor is in the nominal** condition, the detectors should read bulk thermal power times the CPPF. Thus each detector reading, which is actually representative of the flux over a short length, is also equivalent to the power in the potentially hottest channel in the reactor. As the relationship between flux at one point and channel power somewhere else is continually changing due to burnup and refuelling, the calibration of detectors varies continuously. Poor or out-of-date calibration could result in potentially unsafe operation and/or unnecessary reactor trips and is also a nuisance for the operating staff as recalibration must be carried out frequently and manually.

Analog/relay hardware is used in the Bruce NGS-A safety system. Since high-quality relays are becoming increasingly difficult to obtain, they should be phased out of future safety system designs. Meanwhile, computers are becoming more reliable as well as less expensive; they also offer a very high degree of flexibility. This increased flexibility is very important if the algorithms used to decide whether to trip become more complex, i.e. if the safety system is more "intelligent".

One of the operator's main worries is a small margin-to-trip. A more intelligent safety system could alleviate this problem by obtaining a more accurate "measurement" of the maximum channel power and hence allowing a reduction in the error margin required.

1.2 The Intelligent Safety System Project

The basic objective of this project is to develop an Intelligent Safety System for future CANDU reactors (beyond those currently committed) that uses the best information available on the status of the reactor and decides, taking all this information into account, whether to trip. In other words, the trip will be a computed parameter and not simply a one-for-one comparison of readings against fixed trip settings. We consider mainly the problem of fuel melting by overpower. Thus trips based exclusively on process quantities (e.g. boiler level) are assumed to be retained as before, without any change in their algorithms.

The information that is available consists of:

- outputs from self-powered safety detectors of the platinum or Inconel type
- outputs from self-powered mapping detectors of the vanadium type
- outputs from self-powered control detectors of the platinum or Inconel type
- positions (levels) of zone control elements
- positions of adjuster rods
- positions of mechanical control absorbers
- fuel burnup
- bulk thermal power
- instrumented fuel channel powers (flow, temperature, quality)
- inlet header temperatures
- outlet header pressures, and
- pressure drops from inlet to outlet headers.

This paper outlines the mathematical algorithms for processing the information in a logical manner, and a distributed computer architecture applicable to power plants and capable of implementing the algorithms with sufficient speed. For the future, it is our intention to assemble a single channel of such a computer system as a realistic demonstration, and demonstrate and evaluate its effectiveness under many simulated reactor conditions. This demonstration will provide a testing ground for both the algorithms and the reliability of new hardware components.

2. ALGORITHMS

2.1 Flux Mapping

The procedure of flux mapping can be stated generally as follows. A mathematical form for the flux is assumed having M free parameters, and the flux is measured at N locations. If $N = M$, then the equations can be solved exactly; if $N > M$, they can be solved to minimize the errors between the mapped and measured fluxes in a least-squares sense; if $N < M$, they can be solved to minimize the deviations of the free parameters in a least-squares sense. Examples of these three cases are: the bent-plate scheme [1], modal scheme [2], and finite-difference scheme [3], respectively. Philosophically, there are implications of which information is being believed, as shown in Table 1. It is our contention that the measurement must be believed in preference to the mathematical form.

---

* In Bruce NGS-A, some trip settings are adjusted automatically as functions of booster operation.

**Nominal refers to the normal steady-state operating condition with zone levels near 40% full and boosters and control absorbers out.

TABLE 1

PHILOSOPHY OF MAPPING SCHEMES

N = number of detectors

M = number of free parameters

Condition	Example	Detector Readings	Mathematical Form
N = M	Bent-Plate Scheme	believed	believed
N > M	Modal Scheme	not believed	believed
N < M	Finite-Difference Scheme	believed	not believed (excessive parameters included)

The above three schemes are "form-deterministic"; they depend solely on the mathematical forms chosen. There is a fourth method which is dependent on an *a priori* knowledge of a set of answers. In this scheme, a relationship between the inputs and the results is assumed, with a number of free parameters; typically one might choose a matrix (linear) relationship. The free parameters that give the "best" answers are then found; of course, the number of known answers must equal or exceed the number of free parameters. "Best" will typically mean with least-squares error; or in the case of a safety system, it may have a uni-polar (conservative) implication. The ROPT scheme currently employed may be put in this latter category.

We have chosen a mapping scheme of the first type: it is form-deterministic, N = M, and the mapped flux will pass through the measured points. An initial estimate of the flux shape is obtained using a 3-D diffusion equation, for example,

$$\nabla \cdot D\nabla\psi - \Sigma_a\psi + \nu\Sigma_f\psi = 0 \qquad (1)$$

where the reactor physics parameters D, Σ_a and $\nu\Sigma_f$ are obtained using the knowledge of burnup and the device positions. This calculation is not perfect, and the actual flux is given by the calculated shape times a modifying function

$$\phi = f\psi \qquad (2)$$

A form is now assumed for this function

$$\hat{f} = \sum_i F_i r_i^2 \ln r_i^2 + a_o + a_x x + a_y y + a_z a \qquad (3)$$

$$r_i^2 = (x-x_i)^2 + (y-y_i)^2 + (z-z_i)^2 \qquad (4)$$

$$\sum_j F_i = \sum_i x_i F_i = \sum_i y_i F_i = \sum_i z_i F_i = 0 \qquad (5)$$

and the mapped flux is given by $\hat{\phi} = \hat{f}\psi$.

These equations were originally developed as a 2-D interpolant [1]; we have made them 3-dimensional. There is no physical justification for the form chosen* except that it provides a smooth 3-D interpolant with continuous low-order derivatives.

Knowing the fluxes $\tilde{\phi}$ at the detector locations, we can solve equation (2) for the deflections $\tilde{f}$ at the detectors and then equations (3) and (5) for the F values. Substituting back, we can find the fluxes everywhere. In matrix notation, this can be shown to yield

$$\hat{\phi} = C\tilde{f} \qquad (7)$$

The thermal power of a given fuel channel is the weighted sum of the fluxes along that channel,

$$\hat{P}_j = n \sum_k H_{jk}\hat{\phi}_{jk} \qquad (8)$$

where n is initially assumed to be unity and the flux-to-power conversion factor H is burnup dependent. Combining equations (7) and (8) gives, in matrix notation,

$$\hat{P} = E\tilde{f} \qquad (9)$$

Thus equation (7) can be used to find the flux at any desired location in the core while equation (9) maps the measured deflections into the channel powers. Equations (7) and (9) could have been written in terms of measured fluxes, instead of measured deflections, i.e. $\hat{\phi} = C'\tilde{\phi}$ and $\hat{P} = E'\tilde{\phi}$, and the choice is really dependent on programming convenience.

These equations are general and occur irrespective of the actual mapping scheme used; the mapped fluxes and channel powers are linear combinations of the measured fluxes.

2.2 Overall Scheme

The above outlines the basic mapping scheme proposed. However, in our case, some additional features are incorporated. The total scheme is shown schematically in Figure 1. With the reactor at significant

*In 2-D, this form is the equation for the deflection of a plate subjected to transverse forces.

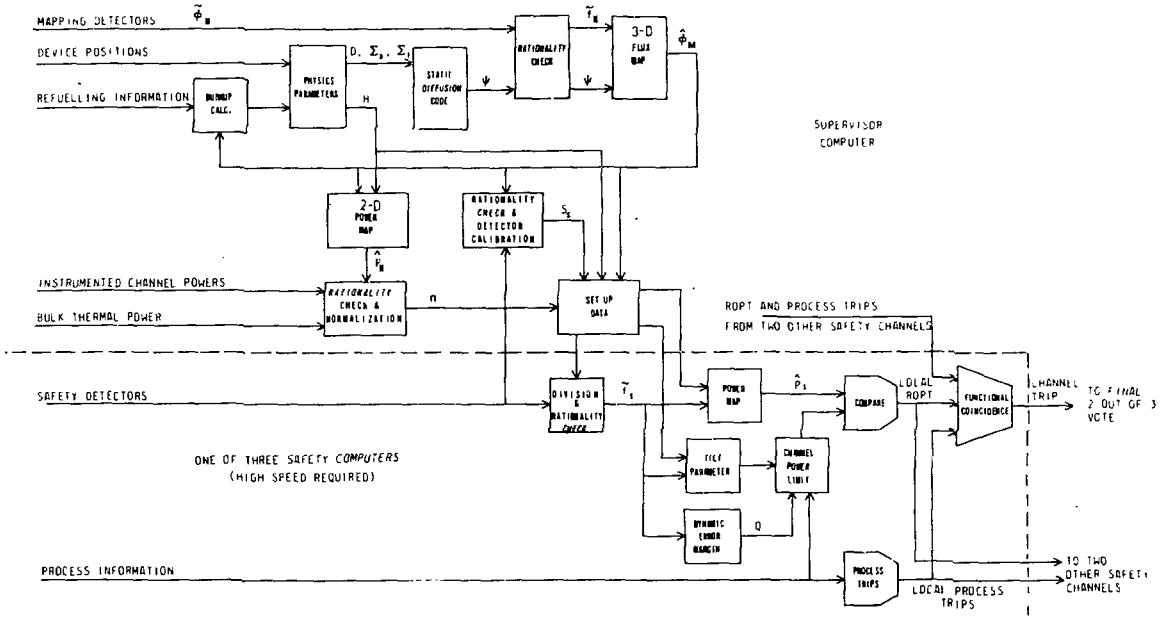

FIGURE 1 PROPOSED ALGORITHM FOR THE INTELLIGENT SAFETY SYSTEM

power, the calculation is begun by accessing the sampled reactivity device positions and obtaining any new refuelling information. From this information, plus the stored burnup data, physics parameters are computed and a theoretical flux distribution, ψ, is obtained, via a diffusion code such as CHEBY [4]. The sampled outputs of the mapping detectors* are accessed and compared to this flux distribution, a rationality check is performed, and any significant deviations are resolved.

The mapping scheme outlined above is then used to produce the mapped flux distribution $\hat{\phi}_M$, using the mapping detector fluxes and equation (7). A mapped power distribution, $\hat{P}_M$, is then obtained using equation (8).

Redundant power information is also available from the instrumented fuel channels and the bulk thermal power measurement. A rationality check is performed and irrational measurements can be dealt with manually. This information is used to obtain a better value for the constant n which was previously assumed to be unity; a weighted least-squares approach is assumed. Filters to match dynamic responses and a rationality check on the value of n are also required. This normalization constant may be thought of as a correction for systematic errors in the absolute detector calibration, the value of H, and/or the ratio of flux in the moderator to that in the fuel.

As the mapping detectors are more accurate than the safety detectors, the sensitivities of the safety detectors are adjusted to force

$$\hat{\phi}_S = \hat{\phi}_M \qquad (10)$$

Again, filtering and a rationality check are required. In simple terms, we are calibrating the platinum safety detectors against the more accurate vanadium mapping detectors.

The flux shape $\hat{\phi}_M$ is then used as the reference flux (replacing ψ) in a second application of the mapping scheme using the safety detectors. With this reference shape and the safety detector sensitivities, the detector outputs of each safety channel can be converted to deflections f_S. Equation (9) can then be applied to give a power map $\hat{P}_S$ based on the safety detector outputs.

An additional feature of our scheme is the dynamic error margin. After a series of studies, we found that the error in the maximum channel power can be correlated to a measurable parameter

$$\varepsilon \geq Q\left(\frac{|f_i - \bar{f}|}{\bar{f}}\right) \leq 0 \qquad (11)$$

*Platinum or Inconel detectors, although relatively prompt responding, are not considered to be as accurate at steady state as vanadium detectors. Thus only the accurate vanadium detectors are included here.

where

$$\varepsilon = \frac{\hat{P}_{max} - P_{max}}{P_{max}} \qquad (12)$$

$$\bar{f} = \frac{1}{N} \sum_{i} f_i \qquad (13)$$

and Q is a negative, simple, piecewise linear function. From this relationship, we obtain

$$P_{max} \leq \frac{\hat{P}_{max}}{1+Q} \qquad (14)$$

Thus the right hand side of equation (14) provides a conservative estimate of the maximum channel power. Alternatively, the factor (1+Q) can be applied to the power limit as shown in Figure 1.

It should be noted that if the reference flux shape is the same as that measured using the safety detectors, then $f_i = \bar{f}$. As $Q(0) \simeq 0$, there is little or no penalty associated with this procedure. However, if the measured and reference flux shapes differ significantly, penalties against "measured" *maximum channel powers* up to 10-15% may be required.

The channel power limit is computed as a function of process variables, a tilt parameter, and dynamic error margin. Comparison with the mapped channel powers yields a local ROPT trip signal. Local process trips are obtained from suitable algorithms. By intercomparing the local trip signals from the three safety computers (see the next section), a two-out-of-three functional coincidence can be determined, and a safety channel trip initiated. A final two-out-of-three ex-computer vote is required to activate the shutdown system.

3. HARDWARE

A long series of calculations was described in the previous section. To produce results rapidly, it is necessary to partition this series into at least two tasks: a fast task that produces a yes/no trip vote and a slow task that produces the parameters for the fast task. The fast task is indicated below the dotted line in Figure 1; the upper portion is the slow task.

The hardware is similarly partitioned, as shown in Figure 2. To obtain the reliability required for reactor safety, triplicated circuits are usually employed. The same philosophy is applied here; the safety computer with its sensors, etc., is triplicated. The safety channel trip decisions of these computers are dealt with via conventional two-out-of-three ex-computer voting logic.

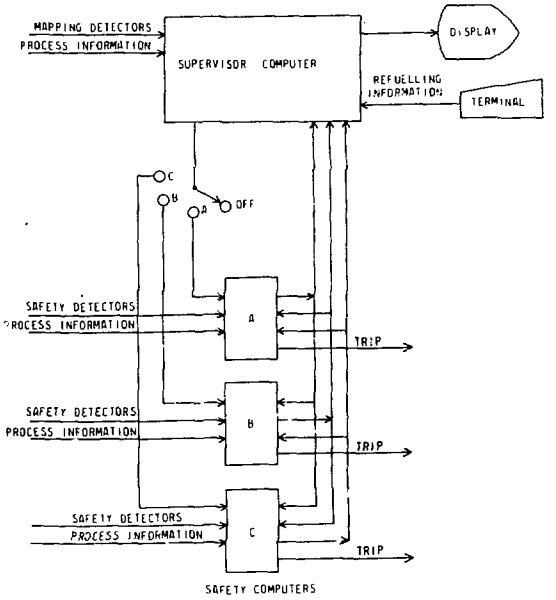

FIGURE 2: SCHEMATIC OF INTELLIGENT SAFETY SYSTEM

The fast task must perform a complete flux mapping calculation which is equivalent to a matrix-vector multiply. This matrix consists typically of 480x20 elements. The reaction time of the safety system to the worst accident must be less than 100 ms, and thus we are aiming for a fast task with a cycle time of ~50 ms. To achieve such a speed, an array processor is required as part of each safety computer.

In contrast, we do not recommend that the slow task be triplicated, as the sensors, computers, etc., become too expensive. The alternative is to manually verify that the slow task is functioning correctly before permitting the data transfer to the fast task, and manually checking for correct data transfer.

The slow or supervisor computer will also perform a number of monitoring functions not shown in Figure 1. For example, it will periodically (say every 5 minutes) monitor the outputs from the safety computers and compare them to similar values calculated from mapping detectors and instrumented fuel channels. This intercomparison of redundant data will lead to rapid diagnosis of failed instruments and/or will indicate that the reference shape is becoming out-of-date.

The interconnections from the supervisor computer to the safety computers and among the safety computers must be fail-safe. Suitable design techniques will ensure that this criterion is met. Watchdog timers (not shown) are also required to ensure that the safety computers are actually operating.

We plan to assemble a demonstration of such a system, consisting of 3 interconnected

computers,

- a supervisor computer,
- a single safety computer with its array processor, analog inputs, and watchdog timer, and
- a computer to simulate the reactor.

The first two will be assembled and programmed in as realistic a manner as possible, so that they could be used directly in a power station. The computer for the reactor simulation will consist of the Hybrid Computer System (Digital Equipment Corp. PDP-11/55 and two Applied Dynamics AD/5 analog computers) presently operational in the Dynamic Analysis Laboratory of the Reactor Control Branch.

This demonstration will provide a testing ground for the proposed algorithms as well as the hardware. The use of computers in safety systems is a new concept for CANDU reactors and their application to this role must be demonstrated. Array processors are relatively new devices with which we are not yet familiar. This demonstration will provide valuable experience with their use, capabilities and reliability. The interconnection of computers is becoming widespread, and new concepts in data transmission, e.g. INTRAN [5], will be examined by means of this demonstration.

4. PROGRESS TO DATE

The mapping scheme outlined above has been examined, and accuracies of 3.5% rms are achievable in computer studies with ~20 detectors. A large number of flux shapes has been examined, and a suitable dynamic margin curve has been obtained.

The scheme calls for the solution of a static diffusion code to provide the reference shape for the flux mapping procedure. The code CHEBY [4] which solves the diffusion equation in 2 energy groups has been converted to run on a PDP-11/55 computer. This exercise shows that it is feasible to run a large diffusion code on a mini-computer. Although running times are considerably slower than on a CDC CYBER 170/6600 system, convergence is achievable in 1-2 hours. Most of this time is spent in transferring data and overlays between the computer memory and disk. We believe that the present generation of mini-computers with large virtual address capability or memory management could produce results in a much shorter time.

5. CONCLUSIONS

An outline has been presented for the design of an Intelligent Safety System for the regional overpower protection of a reactor core. This system breaks with tradition in that it uses a computed value as a trip parameter. The computation is relatively complex as it implicitly contains a full 3-D neutron diffusion calculation blended with a flux mapping procedure. Another new concept is the use not only of computers but also of array processors as essential major elements of the safety system. We have maintained the traditional two-out-of-three arrangement of hardware redundancy.

An attempt has been made to deal in a better way than in the past with redundant information. The guiding principle is that if all the information agrees, then reactor power is allowed to approach the safety limit fairly closely. However, as disagreement increases, a penalty (the dynamic error margin) is applied which lowers the maximum permissible fuel channel power. In this way, either better calibration of instruments or a more accurate and up-to-date calculation will lead to a system having a larger margin-to-trip.

Also, the system is designed to approach an optimum in any steady-state situation. In other words, the dynamic error margin will be a minimum and the margin-to-trip a maximum immediately after downloading of a new matrix from the supervisor computer to the safety computers. If the reactor is in steady state, this condition will persist. Subsequent manoeuvres however will cause some departure in the reactor flux shape from the shape stored in the safety computers. This will increase the uncertainty in the computed fuel channel powers and result in a reduction of the permissible power.

6. REFERENCES

[1] W.E. Gabler and H.D. Fulcher, "Babcock & Wilcox On-Line Computer Advancements in Calculating Uninstrumented Assembly Powers", Presented at ANS-CNA Joint Meeting, Toronto, Ontario, 1976 June 13-18, pp. 4,5,6,7. Also B&W report TP-649.

[2] A.M. Lopez, J.R. Enselmoz and G. Kugler, "Early Operating Experience with the Bruce NGS-A Flux Mapping System", paper in unpublished Atomic Energy of Canada report WNRE-408, 1978 April.

[3] F.N. McDonnell, private communication.

[4] M.H.M. Roshd, "The Physics of CANDU Reactor Design", Presented at the ANS Conference, Toronto, Ontario, 1976 June 14-18, p. 5. Also available as AECL-5803.

[5] A. Capel and G. Yan, "Distributed Systems Design Using Separable Communications", Paper to be presented at the IAEA Specialists' Meeting on Distributed Systems for Nuclear Power Plants, Chalk River, Ontario, 1980 May 14-16.