

USE OF COMBINED SIGNALS
FOR REACTOR SHUTDOWN SIGNAL VALIDATION

by

JUNNE LUNG LIN

Submitted to the Department of Nuclear Engineering on May 6, 1994
in partial fulfillment of the requirements for the Degree of Master of Science

Abstract

A Westinghouse 4-loop PWR is chosen for examination in order to demonstrate the concept of the reactor protection signal validation based upon the effects of systems interactions. The systems interactions and the occurrence of signals during the postulated transients are simulated by using the PRISM code [1]. Based upon the results of the simulations, a set of event-signal matrices corresponding to different plant conditions are constructed and the signals that will lead a certain automatic reactor shutdown signal in appearance in each anticipatory event are identified. These leading signals are utilized in order to validate their associated reactor shutdown signals. Three criteria for the selection of a leading signal as a validation signal are set forth in order to eliminate the common cause failures, to minimize the scale of the required RPS circuit modifications, and to affirm the success of the signal validations for different operational conditions of a nuclear power plant.

After the selection of the validating signals, it is found that seven reactor shutdown signals may be validated by using five leading signals. The required RPS circuit modifications in order to validate reactor shutdown signals based upon the identified validating-validated signal pairs are proposed. Although some of the processes of shutdown signal validation may be dependent upon the reactor power level, the work reported here shows that a single set of signal validation circuits is adequate for use at any reactor power level. The proposed circuit modification is expected to be simple, effective, reliable and low-cost.

As an example of the application of the proposed signal validation method in other areas

where the system interactions can be explicitly identified, the validation of the safety injection signal arising from MSIV's closure is demonstrated and the required circuit modifications are proposed.

The importance rankings among the reactor shutdown signals are established based upon the constructed event-signal matrices. The potential uses of the importance rankings are also discussed.

Based upon the generally satisfactory results of signal validations as well as of operational improvements in the work reported here, it is recommended that the signal validation method based upon system interactions be further investigated more extensively by using more accurate computer codes.

Thesis Adviser : Michael W. Golay
Professor of Nuclear Engineering

Acknowledgments

The author would like to acknowledge the one-year full sponsorship of the Taiwan Power Company, by which the author is employed. The work reported here is one of the efforts of the Taiwan Power Company to provide innovative feedback from operations to the nuclear industry.

Professor M. G. Golay, the advisor of the author, is highly acknowledged. Professor M. G. Golay not only provided wise advice concerning the research direction of the work reported here, but also stimulated the author to solve technical problems arising from the work in every possible aspect. The thinking process in resolving a problem is as important as the solution of the problem itself. This is one of the most valuable lessons the author has learned from Professor M. G. Golay. In addition to the engineering problems, Professor M. G. Golay also help the author express the work reported here in an acceptable fashion in English. Without the help of Professor M. G. Golay, achieving the generally satisfactory results in the work reported here would have been impossible.

The author is indebted to Dr. Shih-Ping Kao, the author of the PRISM code, for his generous help in setting up the PRISM code as well as in providing valuable information about the Westinghouse 4-loop PWRs. Without the PRISM code and the assistance of Dr. Shih-Ping Kao, achieving the generally satisfactory results in the work reported here would be very difficult.

The author would like to recognize Professor David D. Lanning for providing the author many helpful comments which enhanced the content and clarity of the work reported here.

The author would also like to acknowledge the impeccable support received from his colleagues in the Taiwan Power Company. Mr. A. H. Jeng, Director of the Nuclear Safety Department in the Taiwan Power Company, together with the colleagues under his direction, especially Mr. S. H. Huang, Mr. S. C. Chiang, and Mr J. C. Kang, have provided all help which the author requested during the work in a very prompt fashion. Additional strong support from Mr. C. C. Chen, Mr. Golden Chen at the Maanshan Nuclear Power Station, Mr. S. T. Peng reside at INPO, Dr. J. R. Wang at the Institute of Nuclear Energy Research, and Mr. Kevin B. Terry at MIT is highly appreciated. Their support was essential in completing the work reported here.

Finally, the author wishes to acknowledge the encouragement and indulgence of his wife, Lydia Chang, who steadfastly made sure that he was able to work as effectively as possible.

Table of Contents

Title	1
Abstract	2
Acknowledgments	4
Table of Contents	5
List of Tables	8
List of Figures	9
Nomenclatures	10
 Chapter 1: Introduction	 13
 Chapter 2: Signal Validation Technologies Used in the Industry	 15
2.1 Signal Validation Techniques	15
2.1.1 The SGCC Algorithm	16
2.1.2 The MGCC Algorithm	16
2.1.3 The PEM Algorithm	17
2.1.4 The PHC Methodology	17
2.1.5 The BND Algorithm	18
2.2 The Application of the Signal Validation Techniques	19
2.3 Signal Validation Based upon System Interactions	20
2.3.1 System Interactions	20
2.3.2 Some Simple Examples of Use of Method Developed Here Exist in the Operating Nuclear Power Plants	21
2.3.3 A Systematic Study	21
 Chapter 3: The Reactor Shutdown Signal Validation Based upon System Interactions ..	 23
3.1: The Reactor Protection System for Westinghouse Pressurized Water Reactors	23
3.2: The Event-Signal Matrix Based upon the Available Safety Analyses	29
3.2.1: The Events for the Event-Signal Matrix	29
3.2.2: The Signals for the Event-Signal Matrix	31
3.2.3: The Construction of the Event-Signal Matrix Based upon the Available Safety Analyses	32

3.2.4: The Observed System Interactions Based upon the Constructed Event-Signal Matrices-----	32
3.2.5: The Inadequacy of the Event-Signal Matrices Based upon the Available Safety Analyses -----	34
3.3: The Pressurized Reactor Interactive Simulation Model (PRISM)	
Simulation Code -----	35
3.3.1: The Calculations Performed Using PRISM-----	36
3.3.2: The Setup of the PRISM for Constructing the Event-Signal Matrices-----	38
3.4: The Event-Signal Matrix Based upon PRISM Results, with All Control Systems Being Available -----	39
3.4.1: The Constructed Event-Signal Matrix -----	39
3.4.2: The Criteria for Selecting the Validating Signals-----	39
3.4.3: The Pre-selected Validating-validated Signal Pairs -----	41
3.5: The Event-Signal Matrices without All Control Systems Available -----	44
3.5.1: The Combinations of the Control Systems Availabilities-----	44
3.5.2 The Conclusive Validating-Validated Signal Combinations -----	52
3.6 The Validating Signals and the Physical Interpretations of the Validating Processes -----	54
3.6.1 Use of the Steam/Feedwater-Flow-Deviation-Alarm Signal to Validate the Steam Generator-Level-High-Trip or Steam Generator-Level-Low-Low-Trip signal -----	54
3.6.2 Use of the Tav _g /Tref-Deviation-Alarm Signal to Validate the Reactor-Power-High-Trip or Pressurizer-Pressure-Low-Trip Signal -----	54
3.6.2.1 Use of the Tav _g /Tref-Deviation-Alarm Signal to Validate the Reactor-Power-High-Trip Signal-----	55
3.6.2.2 The Validation of the Pressurizer-Pressure-Low-Trip Signal-----	56
3.6.3 Use of Pressurizer-Backup-Heater-Actuation or the Tav _g /Tref-Deviation-Alarm Signal to Validate the Over-Temperature-Delta-Temperature-High-Trip Signal-----	57
3.6.3.1 Use of the Pressurizer-Backup-Heater-Actuation Signal to Validate the Over-Temperature-Delta-Temperature-High-Trip Signal-----	57
3.6.3.2 Use of the Tav _g /Tref-Deviation-Alarm Signal to Validate the Over-Temperature-Delta-Temperature-High-Trip Signal-----	58

3.6.3.3 Use of the Union of the Pressurizer-Backup-Heater-Actuation Signal and the Tavg/Tref-Deviation-Alarm Signal to Validate the Over-Temperature-Delta-Temperature-High-Trip Signal-----	58
3.6.4 Use of the Control Rod-Deviation-Alarm to Validate the Reactor-Power-Positive Rate-High-Trip and the Reactor- Power-Negative Rate-High-Trip Signals-----	59
Chapter 4 : The Applications of the Work Reported Here -----	60
4.1 “Trip” Reduction in the Nuclear Power Plants -----	60
4.1.1 The RPS Logic Modifications -----	60
4.1.1.1 The Modifications for Reactors Operating at 100% RTP -----	60
4.1.1.2 The Modifications for Reactors Operating at Powers Other than 100% of RTP-----	62
4.1.2 The Evaluation of the Logic Modifications -----	64
4.1.2.1 Simplicity and Compatibility -----	64
4.1.2.2 Reliability Considerations -----	64
4.1.2.3 Cost-benefit Considerations-----	65
4.2. Importance Ranking Among the Automatic Reactor Shutdown Signals -----	68
4.2.1 The Estimation of the Automatic Reactor Shutdown Signal Importance Rankings-----	68
4.2.2 The Applications of the Automatic Reactor Shutdown Signal Importance Rankings-----	69
4.3 The Validation of the Safety Injection Signal due to the Steam Line Pressure-Low Signal -----	71
4.3.1 The Impact of an Unintended Safety Injection -----	71
4.3.2 The Unintended Safety Injection due to a MSIV’s Closure -----	71
4.3.3 The Elimination of the Unintended Safety Injection -----	72
Chapter 5: Conclusions and Recommendations -----	75
5.1 Summary-----	75
5.2 Conclusions and Recommendations-----	77
References-----	79

List of Tables

<u>Table Number</u>	page
3.1	Setpoints for controls, alarms, and automatic reactor shutdowns ----- 25
3.2	The event-signal matrix based upon available safety analyses----- 33
3.3	The event-signal matrix based upon PRISM analyses with all control systems being available----- 40
3.4	The pre-selected accompanying signals for different reactor shutdown signals based upon PRISM analyses with all control systems being available ----- 43
3.5.	The event-signal matrix based on PRISM analyses without the OTDT-H-A/B/R control functions being available ----- 46
3.6.	The event-signal matrix based on PRISM analyses without the Rx-PWR-H-A/B control function being available----- 47
3.7.	The event-signal matrix based on PRISM analyses without the automatic rod control being available-----48
3.8.	The event-signal matrix based on PRISM analyses without the automatic steam dump control being available----- 49
3.9.	The event-signal matrix based on PRISM analyses without the automatic PZR pressure (PORV, spray, heaters) and level controls being available----- 50
3.10.	The event-signal matrix based on PRISM analyses without the automatic rod, steam dump, PZR pressure (PORV, spray, heaters) and level controls being available----- 51
3.11	The validating-validated signal pairs based upon the selection criteria----- 53

List of Figures

Figure number	page
3.1	Typical inputs for Westinghouse-PWR reactor protection system----- 24
3.2	Typical instrumentation connections for Westinghouse-PWR reactor protection system----- 28
3.3	Single-loop nodal presentation of the RCS and S/G model in the PRISM program----- 36
4.1	Modified RPS logic circuits for W-PWR operating at 100% of RTP----- 61
4.2	RPS logic modifications for W-PWR operating at any power level -----63
4.3	The Logic Modification for Eliminating Unintended Safety Injection Due to MSIV's closure----- 74

Nomenclature

A = Alarm
AMSAC = ATWS Mitigation System Actuation Circuitry
AOT = Allowed Outage Time
ATWS = Anticipatory Transient Without Scram
B = Control Rod Block
B/H = Backup Heater
BND = Bias and Noise Detection
BOP = Balance Of Plant
C = Close
CLRC = Complete Loss of Reactor Coolant flow
CRDA = Control Rod Drop Accident
CREJ = Control Rod Ejection
Ctrl Rod = Control Rod
Ctrl Rod-D-A = Control Rod-position Deviation-Alarm
CVCS = Chemical and Volumn Control System
D = Deviation
DNB = Departure from Nucleate Boiling
DOBA = Dilution Of Boric Acid during power operation (with rod in manual control)
DSTF = Decrease in Steam Flow (10% turbine load decrease)
DT = Delta Temperature, Temperature Difference between RCS hot leg coolant and RCS cold leg coolant
EDG = Emergency Diesel Generator
ESF = Engineered Safety Features
FSAR = Final Safety Analysis Report
FWLB = FeedWater Line Break in one loop
H = High
I&C = Instrumentation and Control
IFWF = Increase in FeedWater Flow (50% increase in one loop)
INNER = Institute of Nuclear Energy Research in Taiwan
ISTF = Increase in Steam Flow (10% turbine load increase)
L = Low; Level
LL = (level) Low Low
LOCA = Loss Of Coolant Accident

LOEL = Loss Of External Load
 LOFW = Loss Of FeedWater flow (feedwater isolation)
 Main Stm-P-L-SI = Main Steam-Pressure-Low-Safety Injection
 MGCC = Multi-parameter General Consistency Checking
 MSIV = Main Steam Isolation Valve
 MSIV-C = Main Steam Isolation Valve-Closure
 MSLB = Main Steam Line Break in one loop
 MSVC = Main Steam isolation Valve Closure in one loop
 MTBT = Main Turbine Trip without immediately reactor trip
 NR = Negative Rate
 NRC = The Nuclear Regulatory Commission of the United States
 O = Open
 ON = Actuation
 OOPV = Opening Of one Pressurizer safety/relief Valve
 OOSV = Opening Of Steam safety/relief Valve in one loop
 OPDT = Over-Power-Delta-Temperature
 OPDT-H-A/B/R = OPDT-H-Alarm/ control rod Block/ turbine Runback
 OPDT-H-T = Over-Power-Delta-Temperature-High-Trip
 OTDT = Over-Temperature-Delta-Temperature
 OTDT-H-A/B/R = OTDT-H-Alarm/ control rod Block/ turbine Runback
 OTDT-H-T = Over-Temperature-Delta-Temperature-High-Trip
 PEM = Process Empirical Modeling
 PHC = Process Hypercube Comparison
 PLRC = Partial Loss of Reactor Coolant flow (in one loop)
 PORV = Pilot Operated Relief Valve
 PR = Positive Rate
 PRISM = Pressurized Reactor Interactive Simulation Model
 PWR = Pressurized Water Reactor
 Pwr = Reactor Power
 PZR = Pressurizer
 PZR-L-D-A = PZR-L-Deviation-Alarm
 PZR-L-H-A = PZR-L-H-Alarm
 PZR-L-H-T = PZR-Level-High-Trip
 PZR-P-H-A = PZR-P-H-Alarm
 PZR-P-H-T = Pressurizer-Pressure-High-Trip
 PZR-P-L-A = PZR-P-L-Alarm

PZR-P-L-T = PZR-P-Low-Trip

PZR-PORV-O = PZR-Pilot Operated Relief Valve-Open

R = Turbine Runback

RCP = Reactor Coolant Pump

RCS = Reactor Coolant System

RCS-F-L-T = Reactor Coolant System-Flow-Low-Trip

RPS = Reactor Protection System

RTP = Rated Thermal Power

RWST = Refueling Water Storage Tank

Rx = Reactor

Rx-Pwr-H-A/B = Rx-Pwr-High-Alarm/ control rod Block

Rx-Pwr-H-T = Reactor-Power-High-Trip

Rx-Pwr-NR-H-T = Rx-Pwr-Negative Rate-High-Trip

Rx-Pwr-PR-H-T = Rx-Pwr-Positive Rate-High-Trip

S = Signal

S/F = Steam/Feedwater

S/F-F-D-A = Steam/Feedwater-Flow-Deviation-Alarm

SG = Steam Generator

SGCC = Single-parameter General Consistency Checking

SG-L-H-T = Steam Generator-Level-High-Trip

SG-L-L-A = Steam Generator-Level-Low-Alarm

SG-L-LL-T = Steam Generator-Level-Low Low-Trip

SGTR = Steam Generator Tube Rupture in one loop

SI = Safety Injection

T = Trip

Tavg = RCS Coolant Average Temperature

Tavg/Tref-D-A = (T average-T reference)-Deviation-Alarm

T/B = Turbine

T/B-T = Turbine-Trip

Tref = Turbine First Stage Reference Temperature

UCRW = Uncontrolled Rod Withdrawal

W = Westinghouse Electric Co.

Chapter 1: Introduction

Over the last 15 years, unplanned automatic reactor shutdowns have been the subject of increased attention in the nuclear power industry. When automatic reactor shutdowns occur, they frequently are followed by undesirable thermal and hydraulic transients that actuate other safety systems. In addition to the undesired stresses upon equipment and challenges to safety systems of nuclear power plants, a reduction in the margin of safety as well as a loss of plant availability both occur because of these events.

The economic loss due to an unplanned automatic reactor shutdown is estimated to be about \$ 2 million for a 1000 MWe plant for a two-day off-line period, while the reduction of nuclear safety is very difficult to quantify. This estimation is based upon the assumption that the root cause of the automatic shutdown is clear and that there are no special safety concerns identified by the necessary investigations, and that the nuclear power plant resumes its full power operation two days after its shutdown. If the nuclear safety after the automatic shutdown is in doubt, then the investigations and actions required to clarify the safety concerns will always impose a much more serious financial penalty upon the utility than will the automatic reactor shutdown itself. The average annual capacity factor loss due to automatic reactor shutdown resulting from spurious reactor protection system (RPS) signals, for example, was only 0.17% in 1985 and 1986 for the U.S. commercial nuclear power plant. However, they contributed an additional 4.84% due to the Nuclear Regulatory Commission (NRC) investigations [2]. The unplanned automatic reactor shutdowns would not necessarily result in an NRC investigation, but most of the extended outages followed transient events that were analyzed by NRC incident investigation teams.

Over the last 10 years, the nuclear power industry has made considerable progress in continuing to reduce unplanned automatic reactor shutdowns. For example, in 1980 there were an average of 7.4 unplanned automatic reactor shutdowns per unit per 7000 critical hours at U.S. nuclear power generating unit. This average decreased to 1.2 in 1990. However, the trend of the reduction of unplanned automatic reactor shutdown has leveled off since 1990, with the said average, having values 1.2, 1.3, and 1.1 for 1990, 1991, and 1992, respectively, being essentially unchanged over that interval [3].

Among the remaining unintended reactor shutdowns, about 15% of them were attributed to spurious signals in the RPS [4]. As the operating plants age, it is expected that

the spurious signals in the RPS (as well as in other systems) will become more important in causing unintended reactor shutdowns. Therefore shutdown signal validation may play an increasingly important role in reducing the number of unplanned reactor shutdown in the future.

In the work reported here, use of combined signals based upon system interactions for reactor shutdown signal validation is proposed in order to validate the automatic reactor shutdown demands. Other signal validation technologies currently used in nuclear power plants are also discussed and compared with the proposed methodology.

Chapter 2: Signal Validation Technologies Used in the Nuclear Power Industry

Research in the area of signal validation has been extensive. Initial research centered on the most obvious method of signal validation, that of using redundant signals for a given parameter to check for inter-signal consistency [5]. This methodology was quickly expanded to the addition of analytical redundancy and empirical redundancy for the detection of common-cause failures [6]. Current signal validation techniques have been applied on a demonstration basis at experimental reactor as well as commercial nuclear power plants. Signal validation has recently been incorporated into digital reactor control and protection systems. Although the new designed digital control and protection systems have been proposed to be the major instrumentation and control (I & C) for advanced nuclear power reactors, however, they have not been widely applied in the existing nuclear power plants.

This chapter first discusses the signal validation techniques, points out their merits, limitations, and the reasons why they have not been widely used in the existing plants, then briefly discusses the signal validation technique based upon systems interactions proposed here. A method for use of combined signals for reactor shutdown signal validation is systematically developed in Chapter 3 as an example of signal validation based upon system interactions.

2.1 Current Signal Validation Techniques in Use

Currently, at least the following basic signal validation methodologies have been applied to nuclear power plants:

1. Single-parameter generalized consistency checking (SGCC) for redundant measurements [7].
2. Multi-parameter generalized consistency checking (MGCC) for use with simultaneous validation of redundant measurements of multiple parameters and for common-mode failure detection [8].

3. Process empirical modeling (PEM) to detect measurement system drift [9, 10, 11].
4. Process hypercube comparison (PHC) for plantwide signals monitoring [12].
5. Bias and noise detection (BND) for basic signal changes [13].

A brief description of each of the above techniques is given below.

2.1.1 The SGCC Algorithm

The SGCC algorithm is the most basic signal validation technique in nuclear power plants. It guides performance of a systematic checking of the consistency among a set of redundant measurements of a single parameter (for example, the steam pressure at steam line 1). At time instant t , any two like measurements (direct or analytical) $m_i(t)$ and $m_j(t)$ are said to be consistent with each other if

$$|m_i(t) - m_j(t)| \leq d_i + d_j, \quad (2.1)$$

where d_i and d_j are the tolerances of the instruments for measuring m_i and m_j . Whenever the above equation is not satisfied, an inconsistency index for each measurement is incremented. A signal is created to indicate the sensor failure when the inconsistency index for the sensor exceeds a certain value. This algorithm is only applicable to signals having redundant measurements.

2.1.2 The MGCC Algorithm

The MGCC algorithm is essentially an extension of the SGCC algorithm. In the MGCC treatment, several modules using the SGCC algorithms are applied simultaneously to several sets of similar redundant measurements, e.g., the steam pressure at steam line 1, 2, 3, and 4, one for each line. A complex logic performs the evaluation of the cumulative inconsistency indices of all the parameters. The simultaneous consistency checking within one redundant measurement set, and the cross-checking among redundant measurement sets of similar parameters, results in an algorithm capable of detecting and isolating bias and calibration errors and the more complex common-mode degradation of instrument channels. This algorithm is also only applicable to signals with redundant measurements.

2.1.3 The PEM Algorithm

In the PEM algorithm, the process parameters are predicted either by physical modeling or by empirical modeling of a plant subsystem. A certain measured value of a plant parameter then is compared to the predicted values based upon other measured parameters in order to determine its correctness. The physical modeling is developed based on the knowledge of the inter-relations of different system parameters. The empirical models are basically developed using data from different steady-state operation or using a large amount of data from the same steady state operation. In actual applications, several physical or empirical models are needed to be generated, one for each operation regime.

The general form of the empirical modeling is given by

$$y = C_0 + \sum_{i=1}^N C_i f_i(X), \quad (2.2)$$

where

y = parameter to be predicted

$X = \{ x_1, x_2, \dots, x_m \}$

= set of input parameters that affect the behavior of y

$\{ C_0, C_1, \dots, C_N \}$ = set of constant coefficients

$\{ f_i; i=1, 2, \dots, N \}$ = nonlinear polynomial terms.

This algorithm normally needs a sophisticated software package for use to gather and handle a large amount of data, to optimize model selection, and to predict sensor output.

2.1.4 The PHC Methodology

The PHC algorithm basically compares the observed signal set with the pre-established operational states of a nuclear power plant. The concept behind the PHC is somewhat similar to the PEM approach except that the PHC makes a plantwide comparison of the

process parameters, while the PEM treats single parameters. In the PHC algorithm, a hypercube, or multi-dimensional space, data structure is used to store the historical states of plantwide parameters of the valid operational conditions. A hypercube cell is the smallest unit describing a plant state in an n-dimensional space. Each plant parameter is located in one of the divided intervals and constitutes an entity in the n-dimensional space.

The PHC compares the observed signal set with the stored historical states of the plant and determines its correctness. For example, consider a system in which only three parameters (x,y,z) are monitored. Suppose that the signal range of each parameter is divided into five intervals. Further suppose that the historical states of the plant occupy the hypercube cells of numbered (1,1,1), (2,2,2), (3,3,3), (4,4,4), and (5,5,5). Now during the observation consider that a new unobserved state is seen numbered (1,1,5). It is obvious that both the x and y have been observed together before in this combination but that z was observed in a different state. Therefore the true state is probably (1,1,1) and variable z is probably in error. Another example is that of an new unobserved location (5,2,1), the combination of x, y, z which has not existed before and where no combination of any two variables can be found in the stored hypercube. The abnormal signal cannot be identified with a correct plant state in this case.

The hypercube cell size (or resolution) is determined by how the signal ranges of the plant parameters are divided. Small intervals describe the different operating conditions in more detail but require a larger number of cells.

The weak point of the PHC method is that the stored plant states may never completely cover all of the possible operational states. It also needs a high capacity computer to gather, store, and handle a large amount of data, if fine signal resolution is required. Therefore the range of application of the PHC method is limited.

2.1.5 The BND Algorithm

A signal is said to have an anomaly if, during steady-state operation, the deviation in the level of the signal, its root-mean-square value, or its statistical distribution exceeds a preset tolerance. The anomaly of a signal may be characterized by wideband or single-frequency noise, bias error, pulse-type error, non-symmetric distribution, or a change in the signal bandwidth. In the BND algorithm, various signatures, including mean value,

standard deviation, amplitude probability density function, skewness, kurtosis, etc., are computed from high-frequency scanned data samples and compared against specified threshold values. This algorithm is capable of classifying the signal anomaly into bias, pulse, or noise type.

This algorithm is not powerful if the data scan rate is less than the signal noise frequency. On the other hand, if the data scan rate is as high as is needed, only a few signals can be monitored.

2.2 The Application of the Signal Validation Techniques

The signal validation techniques discussed above might have been successful in reducing the automatic reactor shutdowns in the existing nuclear power plants, should they have been applied to the plants. However, these signal validation technologies are not widely used in the existing nuclear power plants. This may be one of the reasons why the downward trend of the plant shutdown frequency, as discussed in Chapter 1, has been leveling off since 1990. The nuclear power plants hesitate to apply the new signal validation techniques partly because the following reasons:

1. The I&C configuration of a plant is required to be changed substantially, depending upon the scale of application of a new technique. The plants have to be shut down for modifications before the new equipment can be put into service.

First of all, signals have to be connected to one or more computers. The verification of the software for applying the techniques is the second task. After the I & C system installation, the new added equipment, including the isolation amplifiers, the wires, the computers, and other components have to be subjected to maintenance. While the benefits of these changes remain to be seen and are uncertain, the costs of the plant shutdowns and the subsequent maintenance is not difficult to estimate and are sure. The costs and the expected benefits of applying a new technique are always a trade-off, and their associated uncertainties induce caution before any plant changes are to be made.

For example, the Tennessee Valley Authority shut down its two units, Sequoyah units 1 and 2, for 23 days in order to replace the aging analog systems with Westinghouse's Eagle 21 Process Protection System in 1990 [14]. When the decision has to be made to

employ a new system, not many plants are willing to or are able to spend such a long time for plant modifications.

2. Even if the signal validation techniques are applied to the plants, the amount of that they reduce the frequency of automatic shutdowns is limited by the following cause:

- a. Human errors.
- b. Component failures causing shutdown signals to be generated.
- c. Instantaneous component malfunctions caused by factors which included blown fuses, water intrusion into the instruments, lightening, and radio interference.

As described earlier, most of those signal validation techniques are intended to detect signal anomalies, they are designed to indicate signal anomalies during steady-state operation. Although they can provide an early warning for sensor failures, and thus, prevent the plant from being automatically shut down, provided that the failures are rectified in a timely manner, they are not considered reliable enough to block the reactor shutdowns due to the causes listed above.

2.3 Signal Validation Based upon System Interactions

In the work reported here, a signal validation methodology based upon system interactions is proposed as an alternative method for signal validation. One of the merits of the proposed method is that it prevents the unnecessary reactor shut downs, and safety coolant injections in an on line fashion. As is discussed in Chapter 4, the required circuit modifications for the proposed signal validation method is expected to be simple, effective and low-cost. This technique can be used for reducing unintended reactor shutdowns, unintended safety injections, and for operational improvements in other areas where the system interactions can be explicitly identified.

2.3.1 System Interactions

A nuclear power plant is made up of many interacting systems, structures, and

components. An action in one part of the plant leads to the actions in others. Systems interaction is not a new subject in the nuclear power industry. However, early work on the study of system interactions stressed the need to ensure their acceptability or to identify the potential existence of unintended and undesirable interactions [15]. In the work reported here, system interactions are utilized as a basis for signal validation.

2.3.2 Some Simple Examples of Use of Method Developed Here Exist in the Operating Nuclear Power Plants

Use of combined signals, based upon system interactions, as a means of signal validation or incident confirmation actually exists in nuclear power plants. For example, in Westinghouse pressurized water reactor (PWR) plants, a steam generator (SG) water level-low low signal (set at 17% of full scale) will shut the reactor down. But a SG water level-low signal (set at 25% of full scale) coincident with steam/feedwater flow-mismatch signal will also shut the reactor down [16]. The concept behind the latter signal is that even though the SG water level has only reached 25% of full scale, the associated steam/feedwater flow-mismatch in the SG will soon lead the component to the 17% of full scale SG water level-low low setpoint.

Another example found in Westinghouse PWR plants is the use of the refueling water storage tank (RWST) water level-low low signal combined with safety injection (SI) actuation signal. This combined signal automatically switches the low-pressure SI pump suction from the RWST to the containment sump as the sources of water [16]. The concept behind this combined signal is straightforward. The SI will lead the RWST level to decrease and the containment sump level to increase should the plant encounter a loss of coolant accident (LOCA). The combined signal confirms that a LOCA is occurring and that the water in the RWST is depleted. However, either the RWST water level-low low or the SI actuation signal is not adequate to switch the low-pressure pump suction sources.

2.3.3 A Systematic Study

Although the method of signal validation based upon system interactions has been sporadically used in the nuclear power industry, a systematic study has not yet been conducted concerning how to utilize it fully.

In the work described here, use of combined signal for reactor shutdown signal validation is systematically developed in Chapter 3 as an example of signal validation based upon system interactions. Since the automatic reactor shutdown signals are the subjects to be validate, the reactor protection system (RPS), in which the reactor shutdown signals are generated, is first discussed.

Chapter 3: The Reactor Shutdown Signal Validation Based on System Interactions

This chapter consists of 6 sections. Section 3.1 describes the configuration of the RPS of a typical Westinghouse PWR, discusses its intended fail-safe design, its vulnerability to spurious signals or operational errors, and points out that the system interaction may be engineered to validate a reactor shutdown signal by means of other accompanying signals. Section 3.2 previews the feasibility of the signal validation with a signal-event matrix based on the available safety analyses. Section 3.3 introduces the PRISM code [1] which is used to identify the relations among plant events and plant signals and to establish the event-signal matrices. Section 3.4 establishes the event-signal matrix based upon results generated using the PRISM code with all the plant control systems available, sets forth three criteria for selecting the validating signals, and pre-selects the validating signals based on the first two selection criteria. Section 3.5 constructs a set of event-signal matrices with the PRISM, checks the pre-selected validating signals against the third selection criterion set forth, and concludes by proposing a set of validating-validated signals. In section 3.6, the validating process and the physical interpretation for each pair of validating and validated signals is discussed and justified.

3.1 The Reactor Protection System for Westinghouse PWR

The Reactor Protection System (RPS) for Westinghouse Electric Co. pressurized water reactors (PWR) monitors numerous system variables such as reactor power level, system pressure, coolant temperature, in order to ensure the diversity of the protection function. If any predetermined parameter limit is exceeded during anticipated operational events, the system initiates a rapid automatic reactor shutdown [16]. The automatic shutdown prevents the reactor from violating the nuclear fuel design limits and damaging the Reactor Coolant System (RCS) pressure boundary. It also assists the Engineered Safety Features (ESF) Systems in mitigating accidents. The fundamental set of parameters to the RPS for a typical 4-loop Westinghouse PWR is shown in Figure 3.1. The setpoints of the parameters for automatic reactor shutdown as well as other control and alarm functions are listed in Table 3.1 [16,17].

The instrumentation of the RPS consists of two redundant trains. Each train is

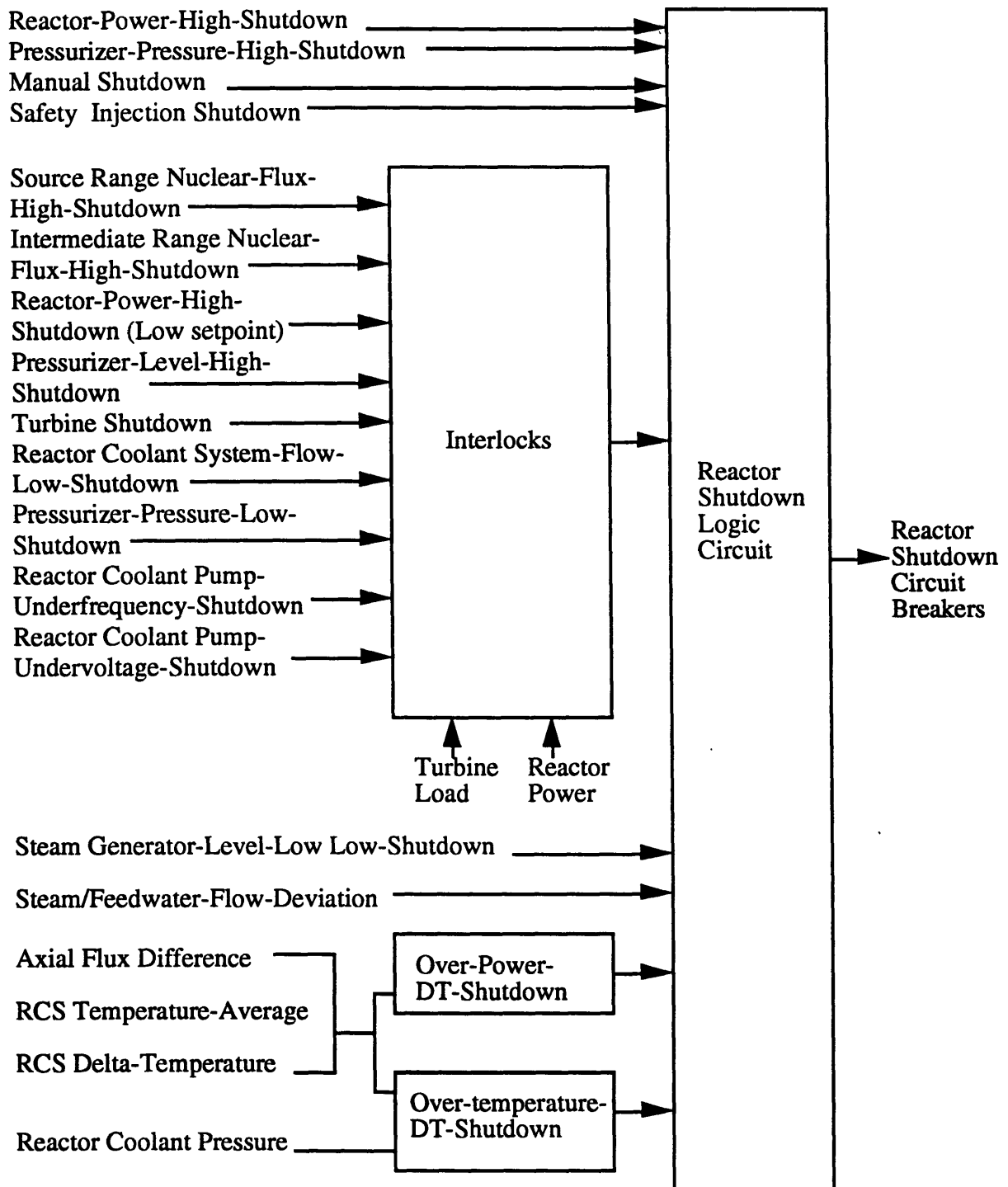


Figure 3.1. Typical Inputs for Westinghouse-PWR Reactor Protection System

Table 3.1. Setpoints for Control, Alarm, and Automatic Reactor Shutdown

<u>Signal</u>	<u>Normal Value*</u>	<u>Setpoint</u>	<u>Function</u>
Rx power high	100% Rated	109% Rated	Reactor shutdown
Rx power high	100% Rated	103% Rated	Alarm and control rod block
PZR pressure high	15.51 Mpa	17.23 Mpa	Reactor shutdown
PZR pressure high	15.51 Mpa	16.20 Mpa	PZR PORV open
PZR pressure low	15.51 Mpa	14.48 Mpa	Alarm
PZR pressure low	15.51 Mpa	13.51 Mpa	Reactor shutdown
PZR pressure low	15.51 Mpa	12.82 Mpa	Safety injection
PZR level high	58% Full scale	92% Full scale	Reactor shutdown
PZR level high	58% Full scale	70% Full scale	Alarm
PZR level deviation	58% Full scale	5% deviation	Alarm
OTDT** high	100% Rated	106% Rated	Reactor shutdown
OTDT** high	100% Rated	103% Rated	Alarm, control rod block and turbine run-back
OPDT** high	100% Rated	107% Rated	Reactor shutdown
OPDT** high	100% Rated	104% Rated	Alarm, control rod block and turbine run-back
Steam/Feedwater flow deviation	0% Rated	5% deviation	Alarm
Tavg/Tref deviation	within 0.83° C	1.1° C deviation	Alarm & control rod movement
S/G level high	50% Full scale	85% Full scale	T/B shutdown, Rx shutdown
S/G level deviation	50% Full scale	5% Full scale	Alarm
S/G level low-low	50% Full scale	17% Full scale	Reactor shutdown
Main steam line pressure low	6.72 Mpa	4.14 Mpa	Safety injection
Reactor power negative rate high	0% Rated/sec	5% Rated/2 sec	Reactor shutdown

<u>Signal</u>	<u>Normal Value*</u>	<u>Setpoint</u>	<u>Function</u>
Reactor power positive rate high	0% Rated/sec	5% Rated/2 sec	Reactor shutdown
Control rod position deviation	0 step	12 steps	Alarm
RCS flow low	100% Rated	90% Rated	Reactor shutdown

****:** the compensated OTDT and OPDT are calculated by:

$$\text{OTDT: } \Delta T \frac{(1 + \tau_{1S})}{(1 + \tau_{2S})} \left[\frac{1}{1 + \tau_{3S}} \right] \leq \Delta T_0 \left\{ K_1 - K_2 \frac{(1 + \tau_{4S})}{(1 + \tau_{5S})} \left[T \frac{1}{(1 + \tau_6)} - T' \right] + K_3(P - P') - f_1(\Delta I) \right\}$$

$$\Delta T \frac{(1 + \tau_{iS})}{(1 + \tau_{sS})} \left[\frac{1}{1 + \tau_{sS}} \right] \leq \Delta T_0 \left\{ K_4 - K_5 \frac{\tau_{iS}}{(1 + \tau_{iS})} \left[\frac{1}{(1 + \tau_e)} \right] T - K_6 \left[T \frac{1}{(1 + \tau_e)} - T \right] - f_2(\Delta I) \right\}$$

T=measured RCS Tavg T'=nominal Tavg at RTP
P=measured PZR pressure P'=nominal RCS operating pressure
s= Laplace transform operator

$K_4=1.09$ $K_5=0.02/^{\circ}\text{F}$ for increasing T_{avg}
 $0/^{\circ}\text{F}$ for decreasing T_{avg} $K_6=0.00128/^{\circ}\text{F}$ when $T>T'$
 $0/^{\circ}\text{F}$ when $T\leq T'$

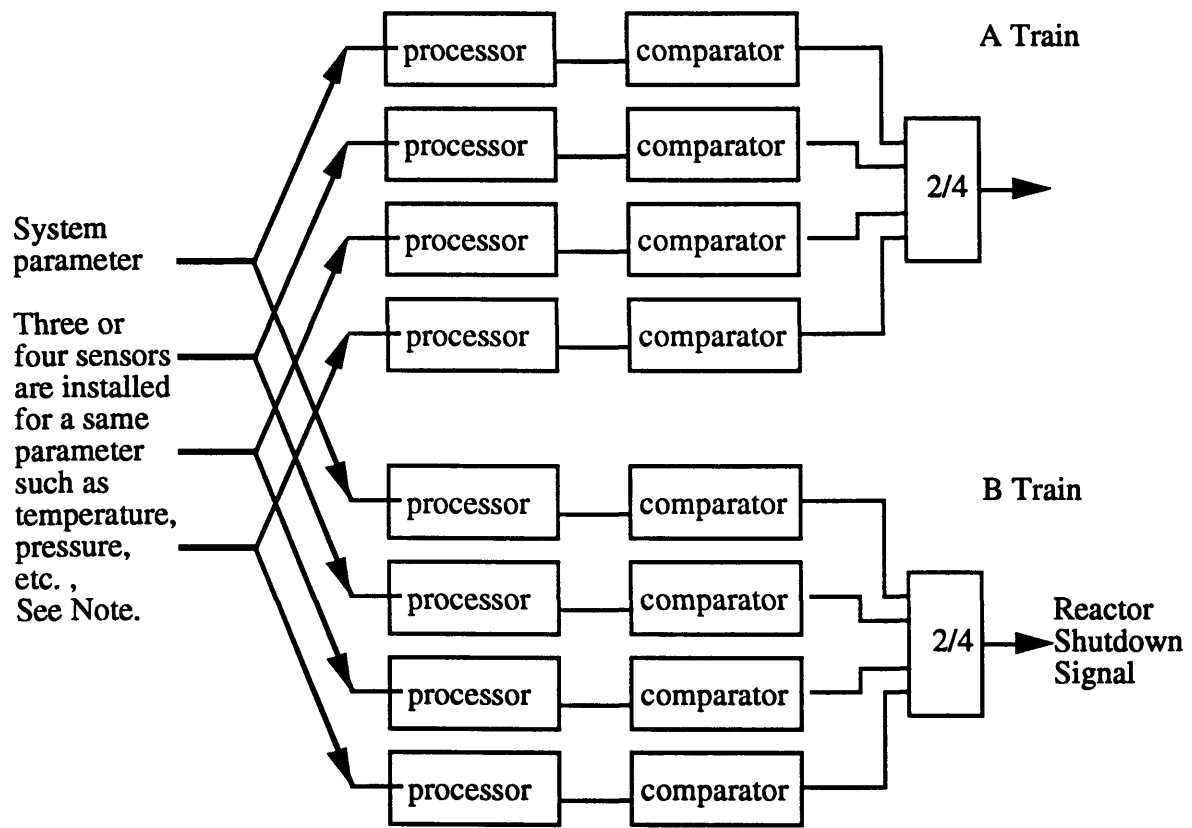
$$f_1(\Delta I) = \begin{cases} 1.26\{35 + (qt - qb)\} & \text{when } qt - qb \leq -35\% \\ 0 & \text{when } -35 < qt - qb \leq 7 \\ -1.05\{(qt - qb) - 7\} & \text{when } qt - qb > 7 \end{cases}$$

Where qt and qb are percent RTP in the upper and lower halves of the reactor core, respectively. $\Delta I = q_t - q_b$, and $q_t + q_b = \text{reactor total power in \% RTP}$.

segmented into four distinct but interconnected modules: the sensors, the signal processors and bistable setpoint comparators, the voting logic blocks, and the reactor shutdown circuits. Three or four sensors are shared by the redundant trains to monitor each input parameter. Each sensor output is connected to its corresponding processor and bistable setpoint comparator in each train. The processor processes the sensed parameter and the comparator compares the processed signal with its preset limit for automatic reactor shutdown. After comparison, the comparator generates a bistable output. This output signal is positive when the limit is exceeded or negative when it is not. It goes to a two-out-of-three or two-out-of-four logic signal voting block. If two or more positive, or trip signals are sensed by the same logic voting block, the block will initiate a rapid automatic reactor shutdown or other appropriate reactor protection operations. Figure 3-2 illustrates the instrumentation connections of the system.

Each RPS instrumentation circuit employs a fail-safe design where a signal malfunction generates a positive signal to the logic voting block. If it is the sensor that is out of order, as is the situation in most cases, then one positive input to the downstream voting block corresponding to this sensor will be generated in both redundant logic voting blocks. Although the two-out-of-three or two-out-of-four logic allows continued operations with a single circuit being failed while continuing to provide the reactor protection function using the remaining active sensors, operating in this condition also leaves the reactor vulnerable to automatic shutdowns due to spurious signals or operator errors.

Since the parameters in the reactor system interact strongly with each other, any reactor shutdown signal is likely to be closely followed by a related signal during a transient. The spurious reactor shutdown signals caused by component malfunctions or operator errors during normal operations will appear alone without any accompanying signal. However, whenever there is a serious event which should cause reactor shutdown, there should be also some other accompanying signals generated. It is possible to use the accompanying signals to validate this reactor shutdown demand. The purpose of the work reported here is to investigate the generality of this proposition and to evaluate the practicality of using it as a basis for increasing the plant operational availability.



Note: Three sensors and two-out-of-three voting blocks are used when the circuits are for protection function only. Four sensors and two-out-of-four voting blocks are used when the circuits are for protection as well as control functions

Figure 3.2. Typical Instrumentation Connections for Westinghouse-PWR Reactor Protection System

3.2 The Event-Signal Matrix Based on the Available Safety Analyses

An event-signal matrix based on readily available safety analyses has first been constructed in order to obtain a preliminary insight into the interactions among the system parameters in different events. The steps for constructing the matrix are fully illustrated after the following basic information is discussed. The readily available safety analyses for the survey of this work consists of the Final Safety Analysis Report (FSAR) for the Maanshan nuclear power station (a twin Westinghouse 3-loop PWR) [17], seven cases of accident analysis performed by the Institute of Nuclear Energy Research (INER) [19~25], and some other cases analyzed by Taiwan Power Company [26~28].

The results of these analyses, which are used to construct the event-signal matrix, are modified to reflect the initial conditions of full power operation. Ideally nuclear power plants should stay mostly at 100% power operation, and avoiding rapid reactor shutdown from full power operation is most desirable in terms of economic considerations as well as for technical reasons such as avoiding thermal-hydraulic impacts, xenon build-up, etc.

3.2.1 The Events for the Event-Signal Matrix

A standard set of safety analyses for a typical nuclear power plant includes about 30 anticipatory events [18]. The event-signal matrices reported here includes 19 events as follows:

<u>Term</u>	<u>Event</u>
IFWF	Increase in <u>Feed</u> <u>Water</u> <u>Flow</u> (50% increase in one feedwater loop)
ISTF	Increase in <u>S</u> <u>t</u> <u>e</u> <u>a</u> <u>m</u> <u>F</u> <u>l</u> <u>o</u> <u>w</u> (10% turbine load increase)
OOSV	<u>O</u> <u>p</u> <u>e</u> <u>n</u> <u>i</u> <u>n</u> <u>g</u> <u>O</u> <u>f</u> <u>S</u> <u>t</u> <u>e</u> <u>a</u> <u>m</u> safety/relief <u>V</u> <u>a</u> <u>l</u> <u>v</u> <u>e</u> in one loop
MSLB	100% <u>M</u> <u>a</u> <u>i</u> <u>n</u> <u>S</u> <u>t</u> <u>e</u> <u>a</u> <u>m</u> <u>L</u> <u>i</u> <u>n</u> <u>e</u> <u>B</u> <u>r</u> <u>e</u> <u>a</u> <u>k</u> in one loop
DSTF	<u>D</u> <u>e</u> <u>c</u> <u>r</u> <u>e</u> <u>a</u> <u>s</u> <u>e</u> in <u>S</u> <u>t</u> <u>e</u> <u>a</u> <u>m</u> <u>F</u> <u>l</u> <u>o</u> <u>w</u> (10% turbine load decrease)
LOEL	<u>L</u> <u>o</u> <u>s</u> <u>s</u> <u>O</u> <u>f</u> <u>E</u> <u>x</u> <u>t</u> <u>e</u> <u>r</u> <u>n</u> <u>a</u> <u>l</u> <u>L</u> <u>o</u> <u>a</u> <u>d</u>
MTBT	<u>M</u> <u>a</u> <u>i</u> <u>n</u> <u>T</u> <u>u</u> <u>r</u> <u>b</u> <u>i</u> <u>n</u> <u>e</u> <u>T</u> <u>r</u> <u>i</u> <u>p</u> without immediate reactor trip
MSVC	<u>M</u> <u>a</u> <u>i</u> <u>n</u> <u>S</u> <u>t</u> <u>e</u> <u>a</u> <u>m</u> isolation <u>V</u> <u>a</u> <u>l</u> <u>v</u> <u>e</u> <u>C</u> <u>l</u> <u>o</u> <u>s</u> <u>u</u> <u>r</u> <u>e</u> in one loop

LOFW	<u>L</u> oss <u>Q</u> f <u>F</u> eed <u>W</u> ater flow (feedwater isolation)
FWLB	<u>F</u> eed <u>W</u> ater <u>L</u> ine <u>B</u> reak in one loop
PLRC	<u>P</u> artial <u>L</u> oss of <u>R</u> eactor <u>C</u> oolant flow (in one loop)
CLRC	<u>C</u> omplete <u>L</u> oss of <u>R</u> eactor <u>C</u> oolant flow
UCRW	<u>U</u> n <u>C</u> ontrolled <u>R</u> od <u>W</u> ithdrawal
CRDA	<u>C</u> ontrol <u>R</u> od <u>D</u> rop <u>A</u> ccident
CREJ	<u>C</u> ontrol <u>R</u> od <u>E</u> jection
DOBA	<u>D</u> ilution <u>Q</u> f <u>B</u> oric <u>A</u> cid during power operation (with rod in manual control)
OOPV	<u>O</u> pening <u>Q</u> f one <u>P</u> ressurizer safety/relief <u>V</u> alve
SGTR	<u>S</u> team <u>G</u> enerator <u>T</u> ube <u>R</u> upture in one loop
LOCA	<u>L</u> oss <u>Q</u> f <u>C</u> oolant <u>A</u> ccident

Other events not included in the event-signal matrix reported here are omitted for the reasons in the following. They are discussed subsequently.

1. Reduction in feedwater flow temperature: The results of the transient are similar to those of the ISTF, but of a reduced magnitude.

2. Main turbine trip with condenser unavailable for steam dump: The transient for this event has been analyzed in MTBT event.

3. Loss of offsite power event: The development of this event may vary in two ways: the electrical generator will either shut-down or not. If the electrical generator shuts-down, the main turbine (T/B) and the reactor coolant pumps (RCPs) will immediately follow it to shut-down, and the reactor will automatically shut-down either on a turbine shutdown signal or on a RCS low flow signal as analyzed in the MTBT and CLRC events. If the electrical generator does not shut down, the plant will actually encounter a LOEL event. Both the cases have been included in the event-signal matrix.

4. Reactor coolant pump rotor seizure (locked rotor): This event is similar to the PLRC event. There will be no other signals available when the reactor shuts-down on a RCS-flow-low signal.

5. Startup of an inactive reactor coolant loop at an incorrect temperature: This event can only happen with one RCP out of service and is allowed only when the reactor power is less than 30%. This is beyond our interest in the work reported here .

6. Other events such as fuel handling accident, etc.: These events are not related to the power operation of a reactor. They have no effect upon reactor shutdown signals.

3.2.2 The Signals for the Event-Signal Matrix

The event-signal matrices reported here include 26 signals as follows:

<u>Term</u>	<u>Definition</u>
OTDT-H-T	<u>O</u> ver- <u>T</u> emperature- <u>D</u> elta- <u>T</u> emperature- <u>H</u> igh- <u>T</u> rip
OTDT-H-A/B/R	OTDT-H- <u>A</u> larm/ control rod <u>B</u> lock/ turbine <u>R</u> unback
OPDT-H-T	<u>O</u> ver- <u>P</u> ower- <u>D</u> elta- <u>T</u> emperature- <u>H</u> igh- <u>T</u> rip
OPDT-H-A/B/R	OPDT-H- <u>A</u> larm/ control rod <u>B</u> lock/ turbine <u>R</u> unback
Rx-Pwr-H-T	<u>R</u> eactor(<u>R</u> x)- <u>P</u> ower- <u>H</u> igh- <u>T</u> rip
Rx-Pwr-H-A/B	<u>R</u> x- <u>P</u> wr- <u>H</u> igh- <u>A</u> larm/ control rod <u>B</u> lock
PZR-P-H-T	<u>P</u> ressurizer- <u>P</u> ressure- <u>H</u> igh- <u>T</u> rip
PZR-P-H-A	<u>P</u> ZR- <u>P</u> - <u>H</u> - <u>A</u> larm
PZR-P-L-T	<u>P</u> ZR- <u>P</u> - <u>L</u> ow- <u>T</u> rip
PZR-P-L-A	<u>P</u> ZR- <u>P</u> - <u>L</u> - <u>A</u> larm
PZR-L-H-T	<u>P</u> ZP- <u>L</u> evel- <u>H</u> igh- <u>T</u> rip
PZR-L-H-A	<u>P</u> ZR- <u>L</u> - <u>H</u> - <u>A</u> larm
PZR-L-D-A	<u>P</u> ZR- <u>L</u> - <u>D</u> eviation- <u>A</u> larm
PZR-PORV-O	<u>P</u> ZR- <u>P</u> ilot <u>O</u> perated <u>R</u> elief <u>V</u> alve- <u>O</u> pen
S/F-F-D-A	<u>S</u> team/ <u>F</u> eedwater- <u>F</u> low- <u>D</u> eviation- <u>A</u> larm
Tavg/Tref-D-A	<u>T</u> average/ <u>T</u> reference- <u>D</u> eviation- <u>A</u> larm
SG-L-LL-T	<u>S</u> team <u>G</u> enerator- <u>L</u> evel- <u>L</u> ow <u>L</u> ow- <u>T</u> rip
SG-L-L-A	<u>S</u> team <u>G</u> enerator- <u>L</u> evel- <u>L</u> ow- <u>A</u> larm
SG-L-H-T	<u>S</u> team <u>G</u> enerator- <u>L</u> evel- <u>H</u> igh- <u>T</u> rip
Main Stm-P-L-SI	<u>M</u> ain <u>S</u> team- <u>P</u> ressure- <u>L</u> ow- <u>S</u> afety <u>I</u> njection
Rx-Pwr-NR-H-T	<u>R</u> x- <u>P</u> wr- <u>N</u> egative <u>R</u> ate- <u>H</u> igh- <u>T</u> rip
Rx-Pwr-PR-H-T	<u>R</u> x- <u>P</u> wr- <u>P</u> ositive <u>R</u> ate- <u>H</u> igh- <u>T</u> rip
Ctrl Rod-D-A	<u>C</u> ontrol <u>R</u> od-position <u>D</u> eviation- <u>A</u> larm
RCS-F-L-T	<u>R</u> eactor <u>C</u> oolant <u>S</u> ystem- <u>F</u> low- <u>L</u> ow- <u>T</u> rip
MSIV-C	<u>M</u> ain <u>S</u> team <u>I</u> solation <u>V</u> alve- <u>C</u> losure
T/B-T	<u>T</u> urbine- <u>T</u> rip

3.2.3 The Construction of the Event-signal Matrix

The event-signal matrix based on the available analyses is shown as Table 3.2. The abbreviations for signals are listed underneath the matrix for quick reference. In each postulated event, the signals which will appear from the beginning of the event up to the point at which the reactor shutdown signal is generated have been identified based on the available analyses. The identified signals are then mapped into the event-signal matrix. For example, in the steam generator tube rupture (SGTR) event, the reactor will be shutdown by the pressurizer-pressure-low-trip (PZR-P-L-T) signal. The leading signals which will appear before the reactor is shut down are the pressurizer-pressure-low-alarm (PZR-P-L-A) signal and the pressurizer-level-deviation-alarm (PZR-L-D-A) signal. Then in the SGTR column of the event-signal matrix, the entity for the shutdown signal PZR-P-L-T is marked as “X”, and the entities for the leading signals PZR-P-L-A and PZR-L-D-A are marked as “O”. This column then represents the results that in a SGTR event, the reactor is shutdown by the PZR-P-L-T signal, and the PZR-P-L-A and PZR-L-D-A signals will be generated before the reactor has been shut down. The “Δ” in the matrix means that the reactor may be shut down by signals other than “X”.

3.2.4 The Observed System Interactions Based upon the Constructed Event-Signal Matrix

From the established event-signal matrix, it is observed that some reactor shutdown signals are always accompanied by other signal(s). For example, OTDT-H-T is always accompanied by Tavg/Tref-D-A; OPDT-H-T always comes along with Rx-Pwr-H-A/B; PZR-P-H-T is closely followed by PZR-L-H-A; S/G-L-LL-T has never appeared alone without the presence of S/F-F-D-A; and Ctrl Rod-D-A has never failed to lead Rx-Pwr-NR-T, etc. This review strongly suggests that one signal can be used to validate another during the transients. Typical results are shown in Table 3.2.

TABLE 3.2: EVENT-SIGNAL MATRIX Based upon Available Safety Analyses

EVENTS	I F W F	I S T F	O S V	M S B	D S F	L O T L	M T B T	M S V C	L O F W	F L B	P L R C	C L R C	U R W	C R D A	C R E J	D O B A	O O P V	S G T R	L O C A
SIGNALS	F	F	V	B	F	L	T	C	W	B	C	C	W	A	J	A	V	R	A
OTDT-H-T	Δ	Δ			Δ	Δ	Δ		Δ							X			
OTDT-H-A/B/R	O	O	O	O	O	O	O		O				O			O			
OPDT-H-T	Δ	Δ	Δ	Δ															
OPDT-H-A/B/R	O	O	O	O															
Rx-Pwr-H-T	Δ	Δ		Δ									X						
Rx-Pwr-H-A/B	O	O	O	O									O			O			
PZR-P-H-T					X	X	X		Δ										
PZR-P-H-A					O	O	O		O										
PZR-P-L-T																	X	X	X
PZR-P-L-A				O													O	O	O
PZR-L-H-T					Δ	Δ	Δ		Δ										
PZR-L-H-A					O	O	O		O	O									
PZR-L-D-A																	O	O	O
PZR-PORV-O																	O		
S/F-F-D-A	Ø			Ø	O	O	O	O	O	O									
Tavg/Tref-D-A	O	O		O	O	O	O	O	O	O						O	O		
SG-L-LL-T									X	X									
SG-L-L-A									O	O									
SG-L-H-T	X																		
Main Stm-P-L-SI				O				Δ											
Rx-Pwr-NR-T														X					
Rx-Pwr-PR-T															X				
Ctrl Rod-D-A														O	O				
RCS-F-L-T											X	X							
MSIV-C				O				O											
T/B-T				X			X	X											

Legend:

X: More Likely Trip Signal

O: Accompanying Signal

Δ: Less Likely Trip Signal

Ø: Accompanying Signal Occurs in Failure Loop

ABBREVIATIONS:

OTDT: Over-Temp. ΔT

OPDT: Over-Power ΔT

Rx-Pwr: Reactor power

PZR: Pressurizer

S/F: Steam/Feedwater

SG: Steam Generator

RCS: Rx Coolant System

RCP: Rx Coolant Pump

MSIV: Main Stm Iso. Valve

-P: Pressure

-L: Level

-F: Flow

-Tavg: RCS Loop Avg Temp

-Tref: T/B Reference Temp.

-H: High

-L: Low

-D: Deviation

-LL: Low Low

-NR: Negative Rate

-PR: Positive Rate

-C: (Valve) Close

-O: (Valve) Open

-A: Alarm

/B: Ctrl Rod Block

/R: T/B Runback

-T: Trip

-SI: Safety Injection

3.2.5 The Inadequacy of the Event-Signal Matrix Based upon the Available Safety Analyses

However, the event-signal matrix based on the readily available analyses alone is not adequate. Most of the available event analyses do not take the functions of the control systems into account [18~28], while the nuclear power plants normally operate with most, if not all, of their automatic control systems being operable. The response and the interactions among the system parameters of a plant with all its automatic control systems being functional could be quite different from that without all automatic control systems working. For example, in a steam generator tube rupture (SGTR) event, the reactor will be shut down by the pressurizer-pressure-low-trip (PZR-P-L-T) signal when its OTDT-H-A/B/R control rod block and turbine run-back function is available, but the reactor will be shut down by the OTDT-H-T signal instead when its OTDT-H-A/B/R function is not available. This is because that the OTDT-H-A/B/R function is designed to reduce the OTDT value by blocking the control rods and running-back the turbine. If the OTDT-H-A/B/R function is not available, the reactor cannot stop the OTDT value from increasing and the OTDT-H-T shutdown setpoint will be reached before the PZR-P-L-T signal can be generated. Different combinations of control functions give different scenarios and thus give different event-signal matrices. In order to factor into the control functions, a complete set of event-signal matrices for a plant with different combinations of control functions should be constructed.

The work reported here was performed as a demonstration of proof-of-concept. It is not intended here to establish a set of definitive event-signal matrices which would apply to a specific plant. Doing this is a large project, involving heavy reliance upon powerful computer codes. The Pressurized Reactor Interactive Simulation Model (PRISM) developed by the Simulation Expert System company was chosen to construct the necessary event-signal matrices in the work described here. The PRISM program can closely simulate plant responses, and is a suitable choice for the demonstration.

3.3 The Pressurized Reactor Interactive Simulation Model (PRISM) Simulation Program

The PRISM is an integrated RCS and S/G thermal hydraulic model developed for real-time simulation for a PWR plant [1]. It incorporates a RCS model derived from the SPK code [29], a U-tube steam generator model (derived from a horizontal steam generator model [30]), a point kinetics model, and a graphic-user-interface, all running under the DOS operating system on a personal computer.

Figure 3.3 illustrates the single-loop representation of the RCS and steam generator model in the PRISM. The reactor vessel is divided into four control volumes for the upper and the lower plenum, the reactor core, and the upper head. Each RCS loop consists of control volumes for the hot leg, the primary side of the U-tube steam generator, and the cold leg. The pressurizer is presented by a vapor region and a liquid region. The secondary side of the steam generator consists of three control volumes for the downcomer, the riser, and the steam dome.

3.3.1 Calculations Performed Using the PRISM Program

The PRISM program allows the user to select at most eleven different malfunctions or accidents, as follows:

- Automatic reactor shutdown
- Main turbine trip
- Reactor fails to automatic shutdown
- Loss of offsite power
- Main feedwater isolation
- Emergency feedwater isolation
- Main steam line isolation (up to four loops)
- Small-break (up to three inches of diameter for each loop) in RCS cold leg
- Steam generator tube rupture (up to three tubes for each steam generator)
- Main steam line break (up to 100% break for each loop)
- Main feedwater line break (up to 100% break for each loop).

36

The PRISM program also provides ten process controllers for the RCS and seven for balance of plant (BOP) systems for different combinations of control functions. The controllers for RCS can be manipulated to control the following functions or properties:

- Control rod drive
- Boron concentration
- Chemical and Volume Control System (CVCS) charging
- CVCS letdown
- Pressurizer proportional heaters
- Pressurizer backup heaters
- Pressurizer Pilot Operated Relief Valves (PORVs)
- Reactor Coolant Pumps (RCPs)
- Safety injection

For the BOP systems, the seven controllers can be used to control the following components or systems:

- Main turbine (turbine control valve)
- Condenser steam dump
- Main steam isolation valves
- Atmospheric steam dump valves
- Main feedwater control valves
- Feedwater control bypass valves
- Auxiliary feedwater control

In addition to the malfunction demands and the controller operations, the input data file for the PRISM can also be modified to alter or disable the control or protection functions.

With the demand of plant malfunctions or accidents, the manipulation of the RCS and BOP controllers, and the modification of the input data file, the PRISM allows the user to simulate plant responses for a wide variety of conditions ranging from operational transients to breach of the RCS pressure boundary.

3.3.2 The Setup of the PRISM

In the simulations performed, the initial reactor power is set at 100% of rated thermal power (RTP) in each case of simulation with the reactor protection and control settings set as listed in Table 3.1.

Although the PRISM provides a wide variety of simulations, some anticipatory events designated in the FSAR have exceeded the normal simulation domain of PRISM. It is necessary to simulate these events using alternative methods. These events include the following:

<u>Term</u>	<u>Event and its simulation</u>
IFWF	30% feedwater flow increase in one loop (this is the maximum the PRISM can simulate in 100% power)
ISTF	10% steam flow increase in all steam loops, which is simulated by 10% steam line breaks in all loops (the turbine controller in PRISM can only bring the turbine up to 100% load)
LOEL	Loss of external load, which is simulated by turbine shutdown without reactor shutdown with steam dump in automatic control if not otherwise specified
CRDA	Control rod drop accident, which is simulated by the addition of boric acid in the RCS
CREJ	Control rod ejection, which is simulated by the subtraction of boric acid in the RCS
LOCA	Loss of coolant accident, the break size of which is limited by the PRISM to less than two inches of diameter in RCS cold leg

During each simulated event, an indication would be given whenever an actuation, alarm or reactor shutdown signal is generated. The generated signals and their times of occurrence have been recorded and have served to be the entities of each event-signal matrix.

3.4 The Event-signal Matrix Based upon PRISM Results, with All Control Systems Being Available

3.4.1 The Constructed Event-signal Matrix

The event-signal matrix based on the simulations performed using the PRISM, with all control systems being available, is shown in Table 3.3. Based upon this event-signal matrix, it is observed that most of the reactor shutdown signals are accompanied by a number of leading signals, while some of them have none. For those that have one or more leading signals, the validation of reactor shutdown signal based on system interactions seems feasible. However, for those that have no leading signal, such as RCS-F-L-T, the validation of reactor shutdown signal based on system interactions seems impossible. One of the eventual purposes of the work described here is to indicate a method for justifying modification of the RPS logic circuits in the existing plants. It is seen from these results that the selection of the validating signals from the leading signals for each reactor shutdown signal can not be arbitrary.

3.4.2 The Criteria for Selecting the Validating Signals

The practical considerations involved in the selection of the validating signals require that the modifications of the RPS logic circuits based upon the selected validating signals should be simple, effective, reliable. In addition, the modifications should not adversely affect the functions of the existing systems.

The criteria set forth for the selection of the validating signals for each reactor shutdown signal are as follows:

1. The validating signals and the reactor shutdown signal to be validated should be generated from different sensors, and it would better if were from different areas in the plant, in order to avoid common-mode-failures. Take the SGTR event as an example again, although the pressurizer-pressure-low-alarm (PZR-P-L-A) signal always leads the pressurizer-pressure-low-trip (PZR-P-L-T) signal, it is inadequate to use the PZR-P-L-A signal to validate the PZR-P-L-T signal. This is because these two signals share the same sensors and signal processors. Thus, it is likely to have the spurious PZR-P-L-A and the

TABLE 3.3 : The Event-signal Matrix Based upon PRISM Analyses
with All Control Systems Being Available.

EVENTS	I F W F	I S T F	O S V	M S B	D S F	L T L	M T T	M S C	L O W	F L B	P L C	C L C	U R W	C R A	C R J	D O A	O O V	S G P R	L O C
SIGNALS																			
OTDT-H-T																X	X		
OTDT-H-A/B/R		O	O										O			O	O	O	O
OPDT-H-T																			
OPDT-H-A/B/R																			
Rx-Pwr-H-T													X						
Rx-Pwr-H-A/B													O						
PZR-P-H-T																			
PZR-P-H-A						O	O												
PZR-P-L-T																		X	X
PZR-P-L-A																		O	O
PZR-L-H-T																			
PZR-L-H-A						O	O												
PZR-L-D-A						O	O		O				O			O		O	O
PZR-PORV-O						O	O		O				O				O		
S/F-F-D-A	Ø			O		O	O		O	Ø									
Tavg/Tref-D-A		O	O		O	O	O		O				O			O	O	O	O
SG-L-LL-T									X	X									
SG-L-D-A	Ø	O	Ø			O	O		O	Ø									
SG-L-H-T	X																		
Main Stm-P-L-SI				O				O											
RX-PWR-NR-H-T														X					
RX-PWR-PR-H-T															X				
Ctrl Rod-D-A														O	O				
RCS-F-L-T											X	X							
MSIV-C				O				Ø											
STM-DUMP-V-O					O	O	O												
T/B-T				X			O	X											

Legend:

X: Reactor Trip Signal

O: Accompanying Signal

Ø: Accompanying Signal Occurs in Failure Loop

Abbreviations:

OTDT: Over-Temp. ΔT

OPDT: Over-Power ΔT

Rx-Pwr: Reactor power

PZR: Pressurizer

S/F: Steam/Feedwater

SG: Steam Generator

RCS: Rx Coolant System

RCP: Rx Coolant Pump

MSIV: Main Stm Iso. Valve

-P: Pressure

-L: Level

-F: Flow

-Tavg: RCS Loop Avg Temp

-Tref: T/B Reference Temp.

-H: High

-L: Low

-D: Deviation

-LL: Low Low

-NR: Negative Rate

-PR: Positive Rate

-C: (Valve) Close

-O: (Valve) Open

-A: Alarm

/B: Ctrl Rod Block

/R: T/B Runback

-T: Trip

-SI: Safety Injection

PZR-P-L-T signals simultaneously. Of course we cannot use the false PZR-P-L-A signal to “validate” the false PZR-P-L-T signal. This consideration has largely ruled out the use of alarm signals which share the same sensors with the reactor shutdown signals.

2. Whenever there is a common leading signal for different reactor shutdown signals, it should be preferentially chosen for validation use in order to reduce the scale of circuit modifications as well as the eventual operating costs. For example, in the last two columns of the matrix of Table 3.3, the PZR-L-D-A signal as well as the Tavg/Tref-D-A signal can be selected to validate the PZR-P-L-T shutdown signal in the SGTR and LOCA events. These two signals do not share the same sensors with the PZR-P-L-T signal. However, the Tavg/Tref-D-A signal appears on the event-signal matrix more frequently than does the PZR-P-L-A. It also has the potential to validate the OTDT-H-T and the Rx-Pwr-H-T shutdown signals in other events. Therefore we should choose the Tavg/Tref-D-A instead of the PZR-L-D-A to validate the PZR-P-L-T signal.

3. The validating signals chosen based on Table 3.3, the event-signal matrix for all control functions being available, should survive every credible operational condition of the plant. That is, a signal cannot be used as a validating signal unless it precedes the reactor shutdown signal which it is to validate no matter what the combination of the control functions of the plant may be.

3.4.3 The Pre-selected Validating-Validated Signal Pairs

The pre-selected validating signals according to the first two rules described above are highlighted in squares in the same column of matrix shown in Table 3.4, and also are listed as follows:

<u>Validating signal</u>	<u>Reactor shutdown signal (to be validated)</u>
Steam/feedwater-flow-deviation-alarm (S/F-F-D-A)	Steam generator-level-high-trip (S/G-L-H-T) ,or Steam generator-level-low low-trip (S/G-L-LL-T)
Tavg/Tref-deviation-alarm (Tavg/Tref-D-A)	Over-temperature-delta-temperature-high-trip (OTDT-H-T),or Reactor-power-high-trip (Rx-Pwr-H-T) ,or Pressurizer-pressure-low-trip (PZR-P-L-T)
Control rod-deviation-alarm (Ctrl Rod-D-A)	Reactor-power-positive rate-high-trip (Rx-Pwr-PR-H-T),or Reactor-power-negative rate-high-trip (Rx-Pwr-NR-H-T)

Note that the reactor shutdown on turbine shutdown (T/B-T) signal is excluded from this list. The T/B-T signal can be generated in the secondary system as well as in the primary system in order to protect the turbine itself in most cases. Including the T/B-T signal will involve the analyses for the secondary system. This is beyond our interest at this moment. Note again that the RCS-flow-low-trip (RCS-F-L-T) signal is not included in this matrix for there is no leading signal for it.

TABLE 3.4 : The Pre-selected Accompanying Signals for Different Reactor Shutdown Signals Based upon PRISM Analyses with All Control Systems Being Available

EVENTS	I F W F	I S T F	O S V	M S B	D S F	L O T L	M T B	M S V	L O F W	P L R C	C L R C	U C R W	C R D A	C R E J	D O B A	O O P V	S G T R	L O C A
SIGNALS																		
OTDT-H-T															X	X		
OTDT-H-A/B/R		O	O									O			O	O	O	O
OPDT-H-T																		
OPDT-H-A/B/R																		
Rx-Pwr-H-T												X						
Rx-Pwr-H-A/B												O						
PZR-P-H-T																		
PZR-P-H-A						O	O											
PZR-P-L-T																	X	X
PZR-P-L-A																	O	O
PZR-L-H-T																		
PZR-L-H-A						O	O											
PZR-L-D-A						O	O		O			O			O		O	O
PZR-PORV-O						O	O		O			O				O		
S/F-F-D-A	Ø			O		O	O		O	Ø								
Tavg/Tref-D-A		O	O		O	O	O		O			O			O	O	O	O
SG-L-LL-T									X	X								
SG-L-D-A	Ø	O	Ø			O	O		O	Ø								
SG-L-H-T	X																	
Main Stm-P-L-SI				O				O										
RX-PWR-NR-H-T													X					
RX-PWR-PR-H-T														X				
Ctrl Rod-D-A													O	O				
RCS-F-L-T										X	X							
MSIV-C				O				Ø										
STM-DUMP-V-O					O	O	O											
T/B-T				X			O	X										

Lengend:

X: Reactor Trip Signal;

O: Accompany Signal;

Abbreviation:

OTDT: Over-Temp. ΔT

OPDT: Over-Power ΔT

Rx-Pwr: Reactor power

PZR: Pressurizer

S/F: Steam /Feedwater

SG: Steam Generator

RCS: Rx Coolant System

RCP: Rx Coolant Pump

MSIV: Main Stm Iso. Valve

Ø: Accompany Signal Occurs in Failure Loop

-P: Pressure

-L: Level

-F: Flow

-Tavg: RCS Loop Avg Temp

-Tref: T/B Reference Temp.

-H: High

-L: Low

-D: Deviation

-LL: Low Low

-NR: Negative Rate

-PR: Positive Rate

-C: (Valve) Close

-O: (Valve) Open

-A: Alarm

/B: Ctrl Rod Block

/R: T/B Runback

-T: Trip

-SI: Safety Injection

3.5 The Event-signal Matrices without All Control Systems Being Available

As is described earlier, the pre-selected validating signals for a certain reactor shutdown signal have to survive every credible plant situation. We have to construct different event-signal matrices for different combinations of control functions availability of the plant, and check whether the pre-selected validating signals are still leading their corresponding shutdown signals in appearance in each event-signal matrix.

3.5.1 The Different Combinations of the Control Systems Availabilities

Normally, continued operation at power of a nuclear power plant with some of its automatic control functions being disabled is not prohibited by its technical specifications, since the FSAR does not assume that they will be functional. On the other hand, a nuclear power plant is not allowed to operate at power continually if any one of its credible systems or components, which the FSAR assumes to be operable, is in reality inoperable. Therefore, for a nuclear power plant to operate at power with some control systems inoperable is credible, while operation with any accredited system being inoperable is highly unlikely .

The FSAR normally does not assume the automatic control systems to be operable [18], therefore their failures have to be considered for the purpose of signal validation. The control functions which are performed by the automatic control systems are as follows:

- OTDT-H-A/B/R control rod block and turbine run-back function
- OPDT-H-A/B/R control rod block and turbine run-back function
- RX-PWR-H-A/B control rod block function
- Control rod automatic control
- Automatic steam dump control
- Automatic PZR PORV control
- Automatic PZR pressure (spray and heaters) and level controls
- S/G water level control (feedwater control)

Since the OPDT-H-A/B/R signal is not triggered under the condition of Table 3.3, we see that disabling the OPDT-H-A/B/R control rod block and turbine run-back functions will

not affect the plant behavior at all. Therefore the malfunction of the OPDT-H-A/B/R control functions have been excluded from discussion here. The S/G water level control has also been excluded from discussion because the feedwater control valves employ a fail-close design. The fail-closed feedwater valves isolate the main feedwater from being pumped into the S/G. This is essentially a loss of feedwater event (LOFW) and has already been considered in the event-signal matrices. Therefore the operability of the S/G water level control is not considered here. The operability of the six remaining control functions are expected to affect the plant responses during a transient. Although there are other combinations of the system operability which could be considered, only six event-signal matrices, Tables 3.5 to 3.10, have been established as a demonstration of the necessary analyses. The first four matrices correspond to one control system being inoperable each, the fifth corresponds to the inoperability of the PZR pressure and level control systems, and the last one corresponds to most of the control systems being disabled. The matrices and the plant conditions they are based on are self-explanatory by their titles, as follows:

Table 3.5. The Event-signal matrix based upon PRISM analyses without the OTDT-H-A/B/R control functions being available

Table 3.6. The Event-signal matrix based upon PRISM analyses without the Rx-PWR-H-A/B control function being available

Table 3.7. The event-signal matrix based upon PRISM analyses without the automatic rod control being available

Table 3.8. The event-signal matrix based upon PRISM analyses without the automatic steam dump control being available

Table 3.9. The event-signal matrix based upon PRISM analyses without the automatic PZR pressure (PORV, spray, heaters) and level controls being available

Table 3.10. The event-signal matrix based upon PRISM analyses without the automatic rod, steam dump, PZR pressure (PORV, spray, heaters) and level controls being available

The entities in these event-signal matrices have been shaded if they are different from their corresponding entities on Table 3.3, the event-signal matrix based upon having all control systems available.

TABLE 3.5: The Event-signal Matrix Based upon PRISM Analyses
without the OTDT-H-A/B/R Control Functions Being Available.

EVENTS	I F	I S	O S	M S	D S	L T	M T	M S	L V	F W	P L	C L	U R	C R	C R	D B	O P	S T	L C
SIGNALS	F	T	V	B	F	L	T	C	W	B	R	R	W	A	J	A	V	R	A
OTDT-H-T																	X	X	X
OTDT-H-A/B/R																			
OPDT-H-T																			
OPDT-H-A/B/R		O																	
Rx-Pwr-H-T													X			X			
Rx-Pwr-H-A/B		O	O										O			O			
PZR-P-H-T																			
PZR-P-H-A							O	O											
PZR-P-L-T																			
PZR-P-L-A																			
PZR-L-H-T																			
PZR-L-H-A							O	O											
PZR-L-D-A		O					O	O		O							O	O	O
PZR-PORV-O							O	O		O							O		
S/F-F-D-A	Ø			O			O	O		O	Ø								
Tavg/Tref-D-A		O	O			O	O	O		O			O			O			
SG-L-LL-T										X	X								
SG-L-D-A	Ø	O	Ø				O	O		O	Ø								
SG-L-H-T	X																		
Main Stm-P-L-SI				O				O											
RX-PWR-NR-T														X					
RX-PWR-PR-T															X				
Ctrl Rod-D-A														O	O				
RCS-F-L-T											X	X							
MSIV-C				O				Ø											
STM-DUMP-V-O						O	O	O											
T/B-T				X				O	X										

Legend:

X: Reactor Trip Signal;

O: Accompany Signal;

Ø: Accompany Signal Occurs in Failure Loop

Abbreviation:

OTDT: Over-Temp. ΔT

OPDT: Over-Power ΔT

Rx-Pwr: Reactor power

PZR: Pressurizer

S/F: Steam/Feedwater

RCS: Rx Coolant System

RCP: Rx Coolant Pump

MSIV: Main Stm Iso. Valve

-P: Pressure

-L: Level

-F: Flow

-Tavg: RCS Loop Avg Temp

-H: High

-L: Low

-D: Deviation

-LL: Low Low

-NR: Negative Rate

-PR: Positive Rate

-C: (Valve) Close

-O: (Valve) Open

/B: Ctrl Rod Block

/R: T/B Runback

-T: Trip

-SI: Safety Injection

TABLE 3.6: The Event-signal Matrix Based upon PRISM Analyses without the Rx-Pwr-H-A/B Control Function Being Available

EVENTS	I F W	I S T	O S V	M S B	D S F	L T E	M T B	M S V	L O F	F W L	P R C	C L R	U R W	C R D	C R E	D O B	O O P	S G T	L O C
SIGNALS	F	F	V	B	F	L	T	C	W	B	C	C	W	A	J	A	V	R	A
OTDT-H-T													X			X	X		
OTDT-H-A/B/R			O	O									O			O	O	O	O
OPDT-H-T																			
OPDT-H-A/B/R																			
Rx-Pwr-H-T																			
Rx-Pwr-H-A/B																			
PZR-P-H-T																			
PZR-P-H-A							O	O											
PZR-P-L-T																		X	X
PZR-P-L-A																		O	O
PZR-L-H-T																			
PZR-L-H-A							O	O											
PZR-L-D-A							O	O		O			O			O		O	O
PZR-PORV-O							O	O		O			O						
S/F-F-D-A	Ø			O		O	O		O	Ø									
Tavg/Tref-D-A		O	O		O	O	O		O				O			O	O	O	O
SG-L-LL-T									X	X									
SG-L-D-A	Ø	O	Ø			O	O		O	Ø									
SG-L-H-T	X																		
Main Stm-P-L-SI				O				O											
Rx-Pwr-NR-T														X					
Rx-Pwr-PR-T															X				
Ctrl Rod-D-A														O	O				
RCS-F-L-T											X	X							
MSIV-C				O				Ø											
STM-DUMP-V-O					O	O	O												
T/B-T				X			O	X											

Legend:

X: Reactor Trip Signal;

O: Accompanying Signal;

Ø: Accompanying Signal Occurs in Failure Loop

Abbreviation:

OTDT: Over-Temp. ΔT

OPDT: Over-Power ΔT

Rx-Pwr: Reactor power

PZR: Pressurizer

S/F: Steam/Feedwater

SG: Steam Generator

RCS: Rx Coolant System

RCP: Rx Coolant Pump

MSIV: Main Stm Iso. Valve

-P: Pressure

-L: Level

-F: Flow

-Tavg: RCS Loop Avg Temp

-Tref: T/B Reference Temp.

-H: High

-L: Low

-D: Deviation

-LL: Low Low

-NR: Negative Rate

-PR: Positive Rate

-C: (Valve) Close

-O: (Valve) Open

-A: Alarm

/B: Ctrl Rod Block

/R: T/B Runback

-T: Trip

-SI: Safety Injection

TABLE 3.7: The Event-signal Matrix Based upon PRISM Analyses
without the Automatic Rod Control Being Available

EVENTS	I F W F	I S T F	O S V	M S B	D S F	L O L	M T B	M S V	L O F	F W B	P L R	C L R	U C R	C R D	C R E	D O B	O O P	S G T	L O C
SIGNALS	F	F	V	B	F	L	T	C	W	B	C	C	W	A	J	A	V	R	A
OTDT-H-T		X				X	X									X	X	X	X
OTDT-H-A/B/R		O	O			O	O						O			O	O	O	O
OPDT-H-T																			
OPDT-H-A/B/R																			
Rx-Pwr-H-T													X						
Rx-Pwr-H-A/B													O						
PZR-P-H-T																			
PZR-P-H-A							O	O										O	
PZR-P-L-T																			
PZR-P-L-A																			
PZR-L-H-T																			
PZR-L-H-A							O	O											
PZR-L-D-A		O					O	O		O			O			O		O	O
PZR-PORV-O							O	O		O			O				O	O	
S/F-F-D-A	Ø			O			O	O		O	Ø								
Tavg/Tref-D-A		O	O		O	O	O		O				O			O	O	O	O
SG-L-LL-T									X	X									
SG-L-D-A	Ø	O	Ø				O	O		O	Ø								
SG-L-H-T	X																		
Main Stm-P-L-SI				O				O											
Rx-Pwr-NR-T														X					
Rx-Pwr-PR-T															X				
Ctrl Rod-D-A														O	O				
RCS-F-L-T											X	X							
MSIV-C				O				Ø											
STM-DUMP-V-O					O	O	O												
T/B-T				X			O	X											

Legend:

X: Reactor Trip Signal

O: Accompanying Signal

Ø: Accompany Signal Occurs in Failure Loop

Abbreviation:

OTDT: Over-Temp. ΔT

OPDT: Over-Power ΔT

PZR: Pressurizer

S/F: Steam/Feedwater

SG: Steam Generator

RCS: Rx Coolant System

RCP: Rx Coolant Pump

MSIV: Main Stm Iso. Valve

-P: Pressure

-F: Flow

-Tavg: RCS Loop Avg Temp

-Tref: T/B Reference Temp.

-H: High

-L: Low

-D: Deviation

-LL: Low Low

-NR: Negative Rate

-C: (Valve) Close

-O: (Valve) Open

-A: Alarm

/B: Ctrl Rod Block

/R: T/B Runback

-T: Trip

-SI: Safety Injection

TABLE 3.8: The Event-signal Matrix Based upon PRISM Analyses without the Automatic Steam Dump Control Being Available

EVENTS	I F W F	I S T F	O S V	M S B	D S F	L S T L	M S T C	M S V W	L S F B	P L R C	C L R C	U R W	C R D A	C R E J	D O B A	O O P V	S G T R	L O C A
SIGNALS																		
OTDT-H-T															X	X		
OTDT-H-A/B/R			O	O								O			O	O	O	O
OPDT-H-T																		
OPDT-H-A/B/R																		
Rx-Pwr-H-T												X						
Rx-Pwr-H-A/B												O						
PZR-P-H-T																		
PZR-P-H-A						O	O											
PZR-P-L-T																	X	X
PZR-P-L-A																	O	O
PZR-L-H-T																		
PZR-L-H-A																		
PZR-L-D-A						O	O		O			O			O		O	O
PZR-PORV-O						O	O		O			O				O		
S/F-F-D-A	Ø			O		O	O		O	Ø								
Tavg/Tref-D-A		O	O		O	O	O		O			O			O	O	O	O
SG-L-LL-T						X	X		X	X								
SG-L-D-A	Ø	O	Ø			O	O		O	Ø								
SG-L-H-T	X																	
Main Stm-P-L-SI				O				O										
Rx-Pwr-NR-T													X					
Rx-Pwr-PR-T														X				
Ctrl Rod-D-A													O	O				
RCS-F-L-T										X	X							
MSIV-C				O				Ø										
STM-DUMP-V-O																		
T/B-T				X			O	X										

Legend:

X: Reactor Trip Signal

O: Accompanying Signal

Ø: Accompany Signal Occurs in Failure Loop

Abbreviation:

OTDT: Over-Temp. ΔT

OPDT: Over-Power ΔT

Rx-Pwr: Reactor power

PZR: Pressurizer

S/F: Steam/Feedwater

SG: Steam Generator

RCS: Rx Coolant System

RCP: Rx Coolant Pump

MSIV: Main Stm Iso. Valve

-P: Pressure

-L: Level

-F: Flow

-Tavg: RCS Loop Avg Temp

-Tref: T/B Reference Temp.

-H: High

-L: Low

-D: Deviation

-LL: Low Low

-NR: Negative Rate

-PR: Positive Rate

-C: (Valve) Close

-O: (Valve) Open

-A: Alarm

/B: Ctrl Rod Block

/R: T/B Runback

-T: Trip

-SI: Safety Injection

TABLE 3.9: The Event-signal Matrix Based upon PRISM Analyses without the Automatic PZR Pressure (PORV,Spray,Heater) and Level Control Control Being Available.

EVENTS	I F	I S	O S	M S	D S	L O	M T	M S	L O	F W	P L	C R	U R	C D	C R	D E	O B	O P	S T	L C
SIGNALS	F	T	V	B	F	L	T	C	W	B	C	C	W	A	J	A	V	R	A	
OTDT-H-T																	X	X		
OTDT-H-A/B/R			O	O									O				O	O	O	O
OPDT-H-T																				
OPDT-H-A/B/R																				
Rx-Pwr-H-T													X							
Rx-Pwr-H-A/B													O							
PZR-P-H-T						X	X		X											
PZR-P-H-A						O	O		O											
PZR-P-L-T																			X	X
PZR-P-L-A																			O	O
PZR-L-H-T																				
PZR-L-H-A																				
PZR-L-D-A						O	O						O				O		O	O
PZR-PORV-O													O					O		
S/F-F-D-A	Ø			O		O	O		O	Ø										
Tavg/Tref-D-A		O	O		O	O	O		O				O				O	O	O	O
SG-L-LL-T											X									
SG-L-D-A	Ø	O	Ø			O	O		O	Ø										
SG-L-H-T	X																			
Main Stm-P-L-SI				O				O												
Rx-Pwr-NR-T														X						
Rx-Pwr-PR-T															X					
Ctrl Rod-D-A															O	O				
RCS-F-L-T											X	X								
MSIV-C				O				Ø												
STM-DUMP-V-O					O	O	O													
T/B-T				X			O	X												

Legend:

X: Reactor Trip Signal

O: Accompanying Signal

Ø: Accompany Signal Occurs in Failure Loop

Abbreviation:

OTDT: Over-Temp. ΔT

OPDT: Over-Power ΔT

Rx-Pwr: Reactor power

PZR: Pressurizer

S/F: Steam/Feedwater

SG: Steam Generator

RCS: Rx Coolant System

RCP: Rx Coolant Pump

MSIV: Main Stm Iso. Valve

-P: Pressure

-L: Level

-F: Flow

-Tavg: RCS Loop Avg Temp

-Tref: T/B Reference Temp.

-H: High

-L: Low

-D: Deviation

-LL: Low Low

-NR: Negative Rate

-PR: Positive Rate

-C: (Valve) Close

-O: (Valve) Open

-A: Alarm

/B: Ctrl Rod Block

/R: T/B Runback

-T: Trip

-SI: Safety Injection

TABLE 3.10: The Event-signal Matrix Based upon PRISM Analyses
without Automatic Rod, Steam dump, PZR Pressure
(PORV, Spray, Heater) and Level Controls Being Available.

EVENTS	I F	I S	O S	M S	D S	L O	M T	M S	L O	F W	P L	C L	U C	C R	C R	D O	O O	S G	L O
SIGNALS	W	T	V	B	F	L	T	C	W	B	C	C	W	A	J	A	V	R	A
OTDT-H-T																	X		X
OTDT-H-A/B/R		O	O										O				O	O	O
OPDT-H-T																			
OPDT-H-A/B/R																			
Rx-Pwr-H-T																			
Rx-Pwr-H-A/B																			
PZR-P-H-T		X	X		X	X	X		X			X				X		X	
PZR-P-H-A		O	O		O	O	O		O			O				O		O	
PZR-P-L-T																			
PZR-P-L-A																			
PZR-L-H-T																			
PZR-L-H-A																			
PZR-L-D-A													O					O	O
PZR-PORV-O																	O		
S/F-F-D-A	Ø			O		O	O		O	Ø									
Tavg/Tref-D-A		O	O		O	O	O		O				O				O	O	O
SG-L-LL-T										X									
SG-L-D-A	Ø					O	O		O	O									
SG-L-H-T	X																		
Main Stm-P-L-SI				O				O											
Rx-Pwr-NR-T														X					
Rx-Pwr-PR-T															X				
Ctrl Rod-D-A															O	O			
RCS-F-L-T											X	X							
MSIV-C				O				Ø											
STM-DUMP-V-O					O	O	O												
T/B-T				X			O	X											

Legend:

X: Reactor Trip Signal;

O: Accompany Signal;

Ø: Accompany Signal Occurs in Failure Loop

Abbreviation:

OTDT: Over-Temp. ΔT

OPDT: Over-Power ΔT

Rx-Pwr: Reactor power

PZR: Pressurizer

S/F: Steam/Feedwater

SG: Steam Generator

RCS: Rx Coolant System

RCP: Rx Coolant Pump

MSIV: Main Stm Iso. Valve

-P: Pressure

-L: Level

-F: Flow

-Tavg: RCS Loop Avg Temp

-Tref: T/B Reference Temp.

-H: High

-L: Low

-D: Deviation

-LL: Low Low

-NR: Negative Rate

-PR: Positive Rate

-C: (Valve) Close

-O: (Valve) Open

-A: Alarm

/B: Ctrl Rod Block

/R: T/B Runback

-T: Trip

-SI: Safety Injection

3.5.2 The Conclusive Validating-Validated signal Combinations

From the constructed tables, it is observed that all of the pre-selected leading signals would have otherwise survived had the OTDT-H-A/B/R control functions not been disabled. When the OTDT-H-A/B/R control rod block and turbine run-back functions are removed, the Tav/Tref-D-A signal is no longer leading the OTDT-H-T reactor shutdown signal in appearance during the OOPV, SGTR, or LOCA events. If we only use the Tav/Tref-D-A signal to validate the OTDT-H-T reactor shutdown signal, the reactor will not automatically shutdown on the OTDT-H-T signal since the reactor shutdown signal would be thought a spurious signal in this case. We must search to find another leading signal in order to validate the OTDT-H-T reactor shutdown signal in this case.

Fortunately, further analysis shows that the pressurizer back-up heaters have never failed to be actuated before the OTDT-H-T shutdown signal is generated during the OOPV, SGTR, and LOCA events when the OTDT-H-A/B/R function is disabled. The pressurizer (PZR) back-up heaters are installed to heat the water in the PZR, and therefore help to increase the RCS pressure whenever the RCS pressure is below than 15.34 Mpa [17,18]. During the OOPV, SGTR, or the LOCA accidents, the RCS pressure decreases quickly. The pressurizer back-up heaters are actuated to resist the pressure decrease of the RCS during these accidents. Therefore we can use the actuation of the PZR back-up heaters as another validating signal for the OTDT-H-T reactor shutdown signal.

Add the actuation signal of the PZR back-up heaters, denoted as PZR-B/H-ON, for the validation of OTDT-H-T, we have now a complete set of validating signals for any credible operation condition. The conclusive result is shown in Table 3.11.

Table 3.11 The Validating-Validated Signal Pairs Based upon the Selection Criteria

<u>Leading signal</u>	<u>Reactor shutdown signal</u>
Steam/feedwater-flow-deviation-alarm (S/F-F-D-A)	Steam generator-level-high-trip (S/G-L-H-T) ,or Steam generator-level-low low-trip (S/G-L-LL-T)
Tavg/Tref-deviation-alarm (Tavg/Tref-D-A)	Reactor-power-high-trip (Rx-Pwr-H-T),or Pressurizer-pressure-low-trip (PZR-P-L-T)
Tavg/Tref-deviation-alarm (Tavg/Tref-D-A) or PZR-B/H-ON	Over-temperature-delta-temperature-high-trip (OTDT-H-T)
Control rod-deviation-alarm (Ctrl Rod-D-A)	Reactor-power-positive rate-high-trip (Rx-Pwr-PR-H-T),or Reactor-power-negative rate-high-trip (Rx-Pwr-NR-H-T)

3.6 The Validating Signals and the Physical Interpretations of the Validating Processes

3.6.1 The Validation of the Steam Generator-Level-High-Trip or Steam Generator-Level-Low-Low-Trip signal

The steam/feedwater-flow-deviation-alarm (S/F-F-D-A) signal is proposed to validate the steam generator-level-high-trip (S/G-L-H-T) or steam generator-level-low-low-trip (S/G-L-LL-T) signal. This signal validation process is expected to be independent of the initial power level of the reactor

When the steam flow leaving the steam generator does not match the feedwater flow entering the steam generator, the steam generator level starts to change after a short period of level shrinkage or swell. The steam generator level can reach its high-trip setpoint or low-low-trip setpoint only when its steam flow and its feedwater flow largely deviate from each other in advance of the level deviation. In fact, the S/F-F-D-A is set to alert the operators that the steam generator water level may go too high or too low if actions are not taken to match the two flows.

Since the deviation of the steam and feedwater flows leads the S/G water level to change, one may use the S/F-F-D-A signal to validate the S/G-L-H-T or S/G-L-LL-T signals. Also, the reactor power level has played no role in this validation process. This is desirable as the signal validation should be independent of the initial power level of the reactor.

3.6.2 The Validation of the Reactor-Power-High-Trip or Pressurizer-Pressure-Low-Trip Signal

The Tavg/Tref-deviation-alarm signal is proposed for use to validate the reactor-power-high-trip (Rx-Pwr-H-T) and the pressurizer-pressure-low-trip (PZR-P-L-T) signals. The validation of the Rx-Pwr-H-T by the Tavg/Tref-D-A is expected to be power independent, but this is not the case for the validation of the PZR-P-L-T.

3.6.2.1 Use of the Tavg/Tref-Deviation-Alarm Signal to Validate the Reactor-Power-High-Trip Signal

The Tavg/Tref-D-A signal is an indication of a power imbalance between the primary system and the secondary system. The Tref signal is calibrated to be proportional to the first stage steam pressure in the turbine, and therefore represents the turbine power. The Tavg variable is equal to the average of the temperatures of the coolant entering and leaving the reactor core. It is controlled to be within $\pm 0.83^{\circ}\text{C}$ of the Tref by the reactor control system. Whenever the power produced by the reactor is higher than the power removed by the turbine, the Tavg starts to increase. When Tavg is higher than Tref by more than 0.83°C , the control rods are automatically inserted into the reactor core to adjust the reactor power and bring the Tavg to be within 0.56°C of the Tref. On the contrary, if the reactor power is lower than the turbine power, the control rods are automatically withdrawn until the Tavg is brought to be within 0.56°C of the Tref. The Tavg has a span of 17.5°C , from 291.7°C to 309.2°C corresponding to 0% to 100% of rated thermal power (RTP), during normal power operation. The alarm setting of 1.1°C deviation between Tavg and Tref corresponds to a power imbalance of about 6.3% of RTP between the primary and the secondary coolant systems. Thus, the Tavg/Tref-D-A signal essentially indicates that the reactor power is deviant from the secondary turbine power by at least 6.3% of RTP [1,17,18].

The Rx-Pwr-H-T value is set at 109% of rated thermal power (RTP). The maximum power that the turbine in the secondary side is allowed to produce is 100% of RTP. When the Rx-Pwr-H-T signal occurs, the power deviation between the primary and the secondary coolant systems will be at least as high as 9%. Therefore the Tavg/Tref-D-A signal will precede the Rx-Pwr-H-T signal in occurrence in any case.

When the reactor initially operates at a power level less than 100% of RTP, the power deviation between the reactor and the turbine will be more than 9% of RTP should the Rx-Pwr-H-T signal appear. In this case the Tavg/Tref-deviation-alarm signal will precede the Rx-Pwr-H-T signal in occurrence by more than that of 100% of RTP. That is, the validation of the Rx-Pwr-H-T by the Tavg/Tref-D-A is expected to be applicable at any power level.

3.6.2.2 The Validation of the Pressurizer-Pressure-Low-Trip Signal

The validation of the PZR-P-L-T signal is rather indirect, and is explained as follows. The PZR-P-L-T signal only appears in the SGTR or LOCA events with the OTDT-H-A/B/R control function also being operational. In these cases, the decreased pressurizer pressure engenders the OTDT-H-A/B/R signal earlier because the OTDT-H-A/B/R signal is very sensitive to coolant pressure decrease, as is discussed in the next section. The OTDT-H-A/B/R initiates the turbine run-back, a fast turbine power reduction, and thus generates the Tavg/Tref-D-A signal before the reactor is eventually shut down on the fairly low set pressure of the PZR-P-L-T signal.

The OTDT-H-A/B/R occurs earlier than does the PZR-P-L-T signal in the depressurization scenario, and the OTDT-H-A/B/R will immediately stimulate the Tavg/Tref-D-A signal if the OTDT-H-A/B/R control is functional. Therefore the Tavg/Tref-D-A signal will precede the PZR-P-L-T signal and corresponding demand for reactor shutdown.

However, the PZR-P-L-T signal can occur without occurrence of the OTDT-H-A/B/R signal. As is shown in Table 3.1, the value of OTDT is calculated based upon the reactor power and RCS pressure. As the reactor power decreases, the value of the OTDT-H-A/B/R signal decreases also. When the reactor power becomes too low, the low delta-temperature will instead be generated and will preclude the OTDT-H-A/B/R signal from being produced. Therefore, the validation of the PZR-P-L-T signal by the Tavg/Tref-D-A signal is expected to be applicable only when the reactor power exceeds a certain “threshold” level.

This threshold power level could be established by simulating the SGTR and LOCA events with the OTDT-H-A/B/R control function being operational with different initial reactor power levels. The threshold value of the reactor power is that above that power level where the validation of the PZR-P-L-T signal by the Tavg/Tref-D-A signal is applicable. That is, above the threshold power the OTDT-H-A/B/R, and therefore the Tavg/Tref-D-A, will always precede the PZR-P-L-T signal.

3.6.3 Use of the Pressurizer-Backup Heater-Actuation or the Tav_g/Tref-Deviation-Alarm Signals to Validate the Over-Temperature-Delta-Temperature-High-Trip Signal

It is proposed here to use the union of the pressurizer-backup-heater-actuation (PZR-B/H-ON) and the Tav_g/Tref-D-A signal to validate the Over-temperature-delta-temperature-high-trip (OTDT-H-T) signal. The validation process for the OTDT-H-T is expected to be power independent.

The Over-Temperature-Delta-Temperature (OTDT) initiation value is set to prevent a high heat flux condition involving the nuclear fuel and the coolant in the Departure from Nucleate Boiling (DNB) condition. It assures the heat transfer from the nuclear fuel to the coolant will remain in the nucleate boiling condition and it maintains the fuel temperature in an acceptable range. Generally speaking, the higher is the reactor power and the lower is the RCS pressure, the closer is the DNB regime approach. As is shown in Table 3.1, in practice the OTDT value is calculated such that it has a lower value for a lower RCS pressure or a higher reactor power. That is, either a low RCS pressure or a high reactor power (or, high DT) or both can induce the OTDT-H-A/B/R and the OTDT-H-T signals.

3.6.3.1 Use of the Pressurizer-Backup Heater-Actuation Signal to Validate the Over-Temperature-Delta-Temperature-High-Trip Signal

If the OTDT-H-T is originated from low RCS pressure, as it is in the cases of the OOPV, SGTR, and LOCA events, the depressurization of the RCS will first engender the PZR-B/H-ON signal. Since the PZR-B/H-ON is set at only 0.138 Mpa below the nominal RCS pressure of 15.51 Mpa, the PZR-B/H-ON signal will appear in the very beginning of the depressurization transients. That is, the PZR-B/H-ON signal will well precede the OTDT-H-T signal if the OTDT-H-T signal is caused by a pressure loss.

If the reactor initially operates at a rather lower power level than 100% of RTP, the depressurization of the RCS will still cause the PZR-B/H-ON signal. But the OTDT-H-T signal is less likely to occur when the reactor is at a lower power level. Whether or not the OTDT-H-T signal will be generated, the PZR-B/H-ON signal will appear in the RCS depressurization events at any reactor power level. That is, the validation of the OTDT-H-T signal by the PZR-B/H-ON signal is appropriate for RCS depressurization cases at any power level.

3.6.3.2 Use of the Tavg/Tref-Deviation-Alarm Signal to Validate the Over-Temperature-Delta-Temperature-High-Trip Signal

In cases where the OTDT-H-T is induced from an high reactor power level, the high power condition will incur the Tavg/Tref-D-A signal, which will precede the OTDT-H-T signal as is discussed in section 3.6.2.1.

If the reactor initially operates at a rather lower power than 100% of RTP, the Tavg/Tref-D-A signal will appear fairly early whether the OTDT-H-T will appear or not. That is, the validation of the OTDT-H-T signal by the Tavg/Tref-D-A signal is appropriate for any reactor power level, as the manner discussed in the previous section.

3.6.3.3 Use of the Union of the Pressurizer-Backup-Heater-Actuation Signal and the Tavg/Tref-Deviation-Alarm Signal to Validate the Over-Temperature-Delta-Temperature-High-Trip Signal

The PZR-B/U-ON signal alone is not adequate for the validation of the OTDT-H-T signal, since the RCS will not be depressurized if the OTDT-H-T is incurred at high reactor power (or, high DT). The Tavg/Tref-D-A signal alone is not adequate for validation purposes either. If the OTDT-H-T signal is caused by a low RCS pressure, the Tavg/Tref-D-A signal will not appear until the turbine is run-back in response to the OTDT-H-A/B/R signal. The problem is that the OTDT-H-A/B/R control function is not an accredited function.

However, in any case, either the PZR-B/H-ON signal or the Tavg/Tref-deviation-alarm signal, or both, will precede the OTDT-H-T signal. Consequently, the union of the PZR-B/H-ON signal and the Tavg/Tref-deviation-alarm signal is proposed here for use to validate the OTDT-H-T signal. From this discussion it is seen that the validation process is also independent of the initial power of the reactor.

3.6.4 Use of the Control Rod-Deviation-Alarm Signal to Validate the Reactor-Power-Positive Rate-High-Trip and the Reactor-Power-Negative Rate-High-Trip Signals

The reactor-power-positive rate-high-trip (Rx-Pwr-PR-H-T) provides departure from nucleate boiling (DNB) protection against control rod ejection accidents, while the reactor-power-negative rate-high-trip (Rx-Pwr-NR-H-T) protects against control rod drop accidents.

The control rods for a Westinghouse PWR plant are designed to move in pre-selected banks, and the banks are to move in a pre-selected sequence. Each bank of the control rods is divided into two groups of two or four rods each. The two groups in a bank move sequentially such that the first group is always within one step of the second group in the bank. Deviation of any control rod from its group by more than 12 steps will initiate the control rod-deviation-alarm (Ctrl rod-D-A) signal. If the rod deviation alarm is not operable, the operator is required to take action as required by the technical specifications.

Should a control rod eject or drop, the Ctrl rod-D-A signal will first be initiated before the Rx-Pwr-PR-H-T or the Rx-Pwr-NR-H-T signal is generated. Consequently, the control rod-deviation-alarm signal could validate these two reactor shutdown signals. This signal validation process is expected to be power level independent.

In the past reactor shutdowns have occurred due to the Rx-Pwr-PR-H-T signal arising from the rapid RCS cooldown during the load rejection events [31]. The rapid RCS cooldown added a large amount of positive reactivity into the core, particularly near the end of core life when the moderator coefficients of reactivity become strongly negative. The Japanese PWRs have adjusted their Rx-Pwr-PR-H-T setpoints from 5% to 10% of RTP in order to avoid this kind of reactor shutdown actuation since the Rx-Pwr-PR-H-T shutdown signal is designed for use only in rod ejection events. If the signal validation method proposed here had been employed, the reactor shutdowns could have been stopped as being unnecessary in the load rejection events without the analyses and the setpoint adjustment of the Rx-Pwr-PR-H-T signal.

Chapter 4: The Applications of the Work Reported Here

This chapter discusses three applications of the work reported here. Other potential applications are discussed in the final chapter.

4.1 “Trip” Reduction in the Nuclear Power Plants

One of the ultimate applications of the work reported here is to modify the automatic reactor shutdown logic in the reactor protection system (RPS) in order to reduce the frequency of unintended automatic reactor shutdowns. In this section, the required modifications of the RPS logic are proposed based upon the signal validation processes discussed in Section 3.6. The simplicity and compatibility, the reliability, and the cost-benefit implications of the modifications are also discussed here.

4.1.1 The RPS Logic Modifications

Although some of the processes for shutdown signal validation may be dependent upon the reactor power level, the work reported here shows that the same set of validation signals is adequate for use at any reactor power level. The following discussion first depicts the RPS signal modifications which would be used for reactors operating at 100% of rated thermal power (RTP), and then illustrates the use of these signals at power levels other than 100% of RTP.

4.1.1.1 The Modifications for Reactors Operating at 100% of Rated Thermal Power

The logic circuitry modifications for the RPS of a Westinghouse-PWR operating at 100% of RTP are proposed as shown in Figure 4.1 (a),(b),(c), and (d) and are discussed as follows.

Except for the OTDT-H-T signal, each of the other six automatic reactor shutdown signals, the S/G-L-H-T, the S/G-L-L-T, the Rx-Pwr-H-T, the PZR-P-L-T, the Rx-Pwr-PR-H-T, and the Rx-Pwr-NR-H-T, may each be validated by a single preceding signal. As

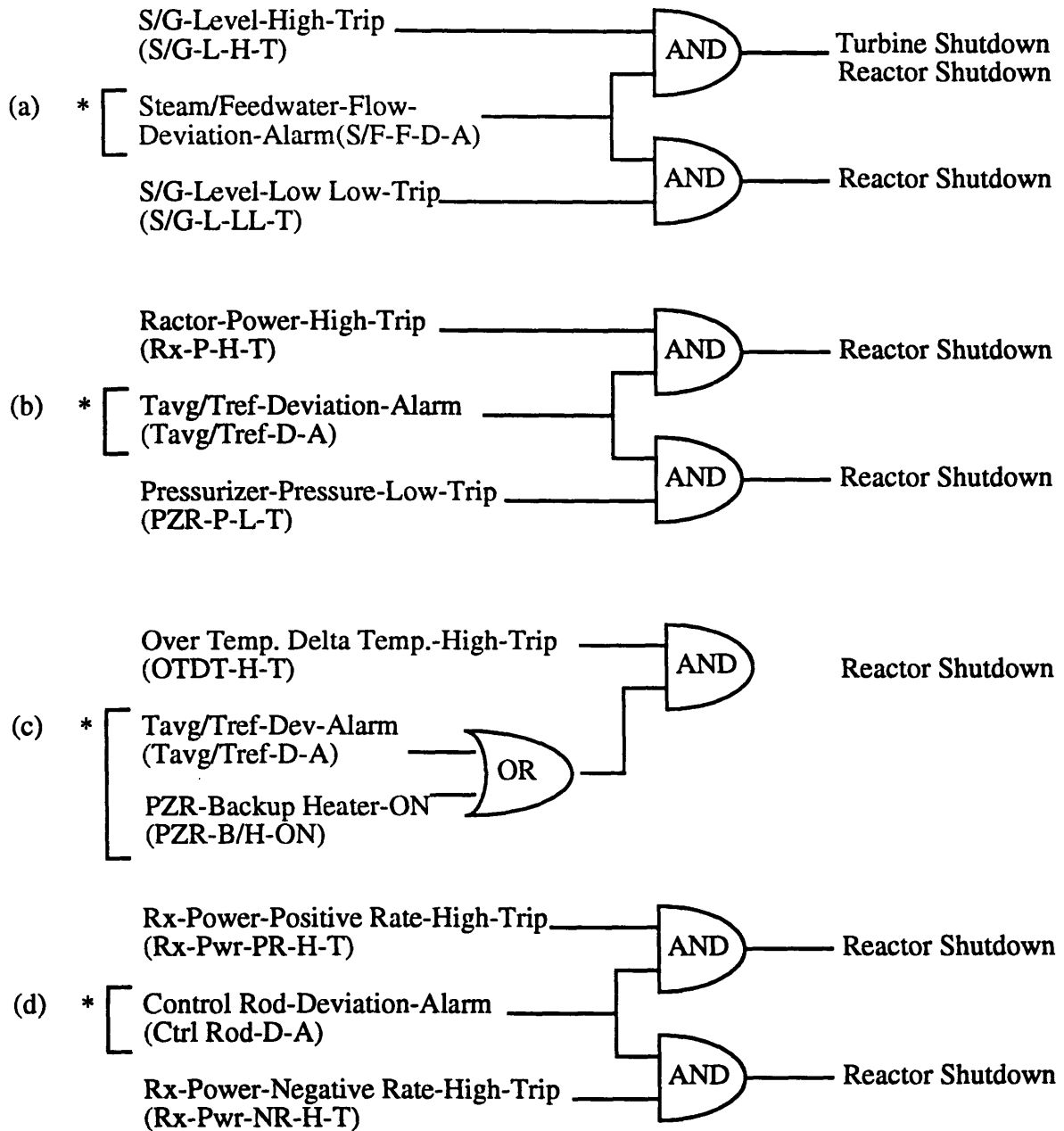


Figure 4.1. Modified RPS logic Circuits for W-PWR operating at 100% of RTP

- (a) Use Steam/Feedwater-Flow-Deviation-Alarm signal to validate Steam generator-Level-High-Trip or Steam generator-Level-Low Low-Trip signal
- (b) Use Tavg/Tref-Deviation-Alarm signal to validate Reactor-Power-High-Trip or Pressurizer Pressure-Low-Trip signal
- (c) Use Tavg/Tref-Deviation-Alarm or Pressurizer-Backup Heater-Actuation signal to validate Over-Temperature-Delta-Temperature-High-Trip signal
- (d) Use Control Rod-Deviation-Alarm signal to validate Reactor-Power-Positive Rate-High-Trip or Reactor-Power-Negative Rate-High-Trip.

* Modified systems input signals are asterisked.

is shown in Figure 4.1 (a), (b), and (d), a Priority AND gate is added to the existing circuit for each of the reactor shutdown signals using one single preceding signal. The Priority AND gate allows the reactor shutdown signal to go to the downstream reactor shutdown actuation circuits only when its corresponding preceding signal has been presented at the AND gate. In this case, the reactor shutdown signal is validated by its validating signal. A reactor shutdown signal without its preceding signal being presented at the AND gate is treated as a spurious signal and will not be forwarded to the downstream circuits. In this manner a spurious reactor shutdown could be stopped by the AND gate as being unnecessary.

For the reactor shutdown signal OTDT-H-T, either the PZR-B/H-ON signal or the Tav_g/Tref-deviation-alarm signal alone is not adequate to validate it. But either the PZR-B/H-ON signal or the Tav_g/Tref-deviation-alarm signal, or both, will precede the OTDT-H-T signal in any case, we need the union of the PZR-B/H-ON signal and the Tav_g/Tref-deviation-alarm signal to validate the OTDT-H-T signal. In this case, an OR gate is used to combine the preceding signals Tav_g/Tref-D-A and PZR-B/H-ON into a single validating signal. An Priority AND gate is then added in like manner as discussed above to validate the reactor shutdown signal OTDT-H-T by means of the combined validating signal.

4.1.1.2 The Modifications Needed for Reactors Operating at Power Levels Other than 100% of Rated Thermal Power

As is discussed in Section 3.6, all but one of the proposed signal validating processes are expected to be independent of the reactor power level. For those that are independent of power, i.e., the validations of the S/G-L-H-T, S/G-L-L-T, Rx-Pwr-H-T, Rx-Pwr-PR-H-T, Rx-Pwr-NR-H-T, and OTDT-H-T signals, the validating circuits as proposed in Figure 4.1 will accomplish the shutdown signal validation for reactors at any power level.

As for the validation of the power dependent PZR-P-L-T signal, a NO gate and an OR gate can be used. As shown in Figure 4.2.(b), the NO gate serves as an interlock which generates a positive output to the OR gate when the reactor power is too low to generate the validating Tav_g/Tref-D-A signal. In this condition, the reactor will be shutdown if the PZR-P-L-T appears alone. This is simply the original shutdown logic. Whenever the reactor power is greater than the threshold power as defined in Section 3.6.2.2, the NO gate

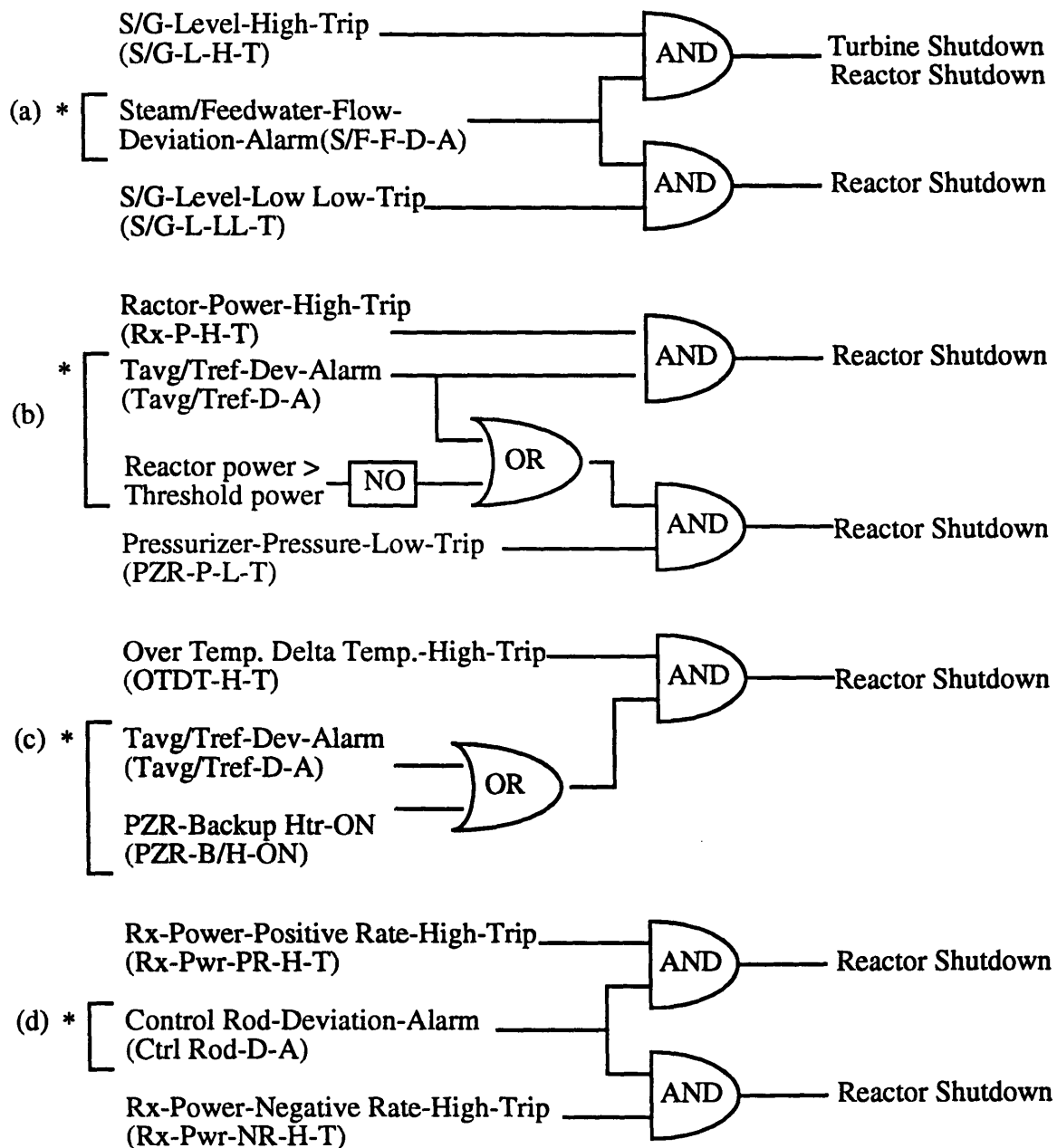


Figure 4.2. RPS logic modifications for W-PWR operating at any power level

(a), (c), and (d) are exactly the same as in Figure 4.1.

(b) A NO gate is used to generate a positive output to replace the missing Tav/Tref-Deviation-Alarm signal when the reactor power level is less than the "threshold power" level. When the reactor power is greater than the threshold power, the NO gate generates a negative output in order to allow the Tav/Tref-D-A signal acting as the validating signal.

* Modified systems input signals are asterisked.

generates a negative output to the OR gate and allows the Tavg/Tref-D-A signal to play a role in validating the PZR-P-L-T signal. This arrangement avoids requiring a different set of validating circuits for use at different reactor power level.

4.1.2 The Evaluation of the Logic Modifications

4.1.2.1 Simplicity and Compatibility

The character of the proposed RPS modification is its simplicity. Only eight Priority AND gates, two OR gates, one NO gate, and some interconnecting wires per RPS train are required to be used in order to accomplish the needed modifications. Keeping a modification simple makes the modification itself more reliable than does a otherwise complicated one.

In a practical design, the electronic components used in these modifications are identical to those in the existing system. The added components are installed in the spare slots inside the instrumentation cabinets, therefore the added components essentially do not occupy an extra space. If this is the case, then the tasks of operation and the maintenance of a modified system is essentially identical to that required prior to the modification. No special care has to be taken to maintain the modified system once the modification is completed. This is one good reason why we suggest modifying the existing reactor protection system instead of using other signal validation techniques.

4.1.2.2 Reliability Considerations

The required RPS modifications proposed here focus on the elimination of spurious reactor shutdown signals in order to reduce the number of unintended reactor shutdowns. Not any signal setpoint for the reactor protection system as well as for the reactor control system needs to be changed. Therefore the results of the safety analyses for a plant which implements the proposed RPS modification would remain valid under this process. No new safety analysis would be needed, except concerning reliability considerations for the new introduced components.

Note that three out of the four validating signals identified in the work reported here, the Tav_g/Tref-deviation-alarm, the PZR-backup heater-actuation, and the control rod-deviation-alarm signals, belong to the reactor control system. Normally, control circuits are not assumed to be functional for purposes of safety analyses. They are not of the same safety grade of design as is the reactor protection system. Therefore two typical considerations have to be addressed in a routine design process to ensure that the use of instrumentation circuits for the validation of the RPS signals will be highly reliable:

1. The instrumentation circuits of the validating signals should be upgraded to “safety-related” quality standards. They should meet the requirements set forth in related documents such as the General Design Criteria, IEEE Standards, etc. That is, they should have independent and reliable power supplies, separated redundant channels, on-line test capability, etc.
2. The instrumentation circuits of the modification should also employ a fail-safe design, where a signal malfunction generates a positive signal to its logic gate. In this manner, the failures of the validating circuits will not impose an adverse effect upon the reliability of the existing reactor protection system.

The nuclear industry has much experience and has developed approved approaches for upgrading components from non-safety grade to safety grade. The first consideration discussed above is not a new issue and is not expected to be a problem for the RPS modifications proposed here. The second consideration discussed above is even more trivial. The existing instrumentation circuits for reactor protection system are already built from a fail-safe design. Thus, the second consideration is not expected to be a problem, especially when the electronic components used in the needed modifications are chosen to be identical to those in the existing system. Involving only three signals and twenty two logic gates being introduced into the existing PRS circuits, the reliability implications of the proposed RPS circuit modifications have been reduced to those of the two solved problems concerning the new introduced components.

4.1.2.3 Cost-benefit Considerations

The costs involved in the implementation of the proposed RPS modifications in a plant may be categorized as follows:

1. The establishment of the event-signal matrices and the identification of the validation-validated signal pairs, over the range of anticipated plant conditions.
2. The design of the modifications of the RPS instrumentation.
3. The safety licensing needed in order to permit the implementation of the proposed RPS modifications.
4. The operation and maintenance of the modified reactor protection system.

If an accurate computer program is used to establish the required event-signal matrices, a reference plant can be chosen as the example upon which to focus all of the initial analyses. The other similarly designed plants can modify the analyses from the reference plant in order to fit their own specific designs. In fact, this is the typical practice used to eliminate the duplication of work and also duplicated costs among the members of different plant Owner's Groups. The design of the needed hardware modifications and the safety licensing of the proposed logic circuit changes can also be standardized in like manner, if it is so desired.

One of the merits of the proposed RPS circuit modifications is that not any setpoint of the existing reactor protection as well as of the control systems is required to be changed. The proposed RPS circuit modifications are used to validate the reactor shutdown signals by means of the accompanying signals which precede the shutdown signals in occurrence. The AND gates added into the existing PRS stop the spurious reactor shutdown signals from being forwarded to the downstream reactor shutdown actuation circuit. Since no signal setpoint in the existing systems has been changed in the development of the proposed circuit modifications, the results of the safety analyses remain unchanged for a plant which would implement the proposed RPS modification. No new safety issue is expected to be involved in order to implement the RPS circuit modifications. As one would expect, the licensing process for a design change without having the results of the safety analyses of the plant changed is more promising than that having the analysis results being changed.

Compared to the amount of installed logic gates and connecting wires in the existing reactor protection system, the added logic gates only account for an increase of the order of

a few percent. The work for this design change is not complicated. The maintenance of the modified system is not expected to impose much a burden upon a plant either, since the modification does not introduce components of types other than those used in the existing system.

The safety licensing cost for this kind of design change for a member of the Owner's Group may be of the order of \$ 0.1 million. This is the amount of money which the Taiwan Power Company, a member of the Westinghouse Owner's Group, paid in 1988 to the Westinghouse Electric Co. for the costs of safety licensing and hardware supplies for the installation of the ATWS Mitigation System Actuation Circuitry (AMSAC) in the Maanshan Nuclear Power Station [32]. The AMSAC is used to actuate the mitigation systems should a PWR plant encounter an anticipated transient without scram (ATWS) situation. The safety licensing costs for the proposed RPS circuit modifications should be of the same order as that of the AMSAC, although the costs of safety licensing vary among different topics. Other information concerning how much the safety licensing costs would be can be drawn from the budgets the Westinghouse Owner's Group has allocated for different topics. These range from several hundred thousands to millions of dollars for different topics [33].

As is estimated in Chapter 1, aside from the other safety impacts, the financial loss is in the order of \$ 2 million for every reactor shutdown. For those which are avoidable these expenses are pure waste. To estimate the cost-benefit of the proposed circuit modifications, assume that a reactor has twenty more years to operate, with an average number of unintended reactor shutdowns due to spurious RPS signals of 0.3 per reactor year. Then the ratio of the marginal benefit to the marginal costs of the employment of the proposed RPS circuit modifications can be calculated by

$$\begin{aligned} \text{marginal benefits} &\sim (0.3 \text{ shutdown per year}) \times (20 \text{ years}) \times (\$ 2 \text{ million per shutdown}) \\ &\sim \$12 \text{ million} \end{aligned}$$

$$\text{marginal costs} \sim \$ 0.1 \text{ million}$$

$$\text{ratio of marginal benefits / costs} \sim (\$12 \text{ million}) / 0.1 \text{ million} \sim 120 !$$

The costs of the analyses for identifying the validating signals and the expenditures for the design of needed hardware modifications are trivial. However, a reduction of the number of unintended reactor shutdown due to spurious signals or operation errors offers a promising opportunity for improving plant safety and economic performance.

4.2. The Importance Rankings Among the Automatic Reactor Shutdown Signals

The event-signal matrices also provide “importance” rankings among the reactor shutdown signals. A reactor shutdown signal which occurs more frequently, and therefore assumes more responsibility for protecting the reactor, is more important than a less frequent one. The event-signal matrices established here provide an exact reactor shutdown signal for each given event. This is not the case in the ordinary safety analyses where the shutdown signal for a given event is always ambiguous [18]. Therefore we can use the established event-signal matrices to estimate the relative frequencies, and hence the importance rankings, among the reactor shutdown signals for protecting the reactor. This section illustrates the estimation of the importance rankings among the reactor shutdown signals based upon the event-signal matrices established in Chapter 3. Some potential applications of the importance rankings are also discussed here.

4.2.1 The Estimation of the Reactor Shutdown Signal Importance Rankings

The estimation of the occurrence frequencies of the reactor shutdown signals is straightforward for a plant if the frequencies the events in the event-signal matrices have been estimated, such as is performed in the Level-1 Probabilistic Risk Assessment (PRA). The expected frequency, P_S , that a given reactor shutdown signal “S” is generated to protect the reactor is simply the summation of the occurrence frequencies P_E of the events in which the reactor is shutdown by the given signal. That is

$$P_S = \sum_i P_{E_i}, \text{ where } i \text{ denotes the } i\text{-th event in which the reactor is shutdown by the given signal}$$

As an illustration, if the occurrence frequencies of the events in the event-signal matrices established in Chapter 3 are assumed to be equal (this is not true, of course), then the relative frequency of a given shutdown signal shutting down the reactor is simply its total number of appearance on all the event-signal matrices. The total numbers of times that the reactor shutdown signals appear on the event-signal matrices, shown in Tables 3.4 to 3.10, are listed as follows:

<u>Reactor Shutdown Signal</u>	<u>Count</u>
OTDT-H-T	21
OPDT-H-T	0
Rx-Pwr-H-T	6
PZR-P-H-T	12
PZR-P-L-T	8
PZR-L-H-T	0
SG-L-LL-T	14
SG-L-H-T	7
Rx-Pwr-NR-H-T	7
Rx-Pwr-PR-H-T	7
RCS-F-L-T	14
T/B-T	14

It is seen that these relative usage frequencies differ from each other significantly among the reactor shutdown signals, with the OTDT-H-T signal counted to a maximum of 21 occurrences but the OPDT-H-T and the PZR-L-H-T signals not appearing. It is obvious that the OTDT-H-T shutdown function assumes much more responsibility for shutting down the reactor than does either the OPDT-H-T or the PZR-L-H-T signal.

4.2.2 The Applications of the Reactor Shutdown Signal Importance Rankings

The expected frequencies of reactor shutdowns by the automatic shutdown signals are very useful to know. Use of more signals not only can provide more complete knowledge for understanding the role in assuring the reactor safety of the reactor shutdown signals which would be provided by the shutdown signal importance rankings. They could also help in plants decisions for allocating limited resources. Furthermore, the operation and maintenance of the reactor protection system may be adjusted based upon the reactor shutdown signal importance rankings.

As is discussed in Chapter 3, the control systems of a nuclear power plant are normally assumed to be inoperable for the purposes of safety analyses. But in reality most if not all, of the control systems of the plant will be operable. One may obtain a biased understanding

of this from the ordinary safety analyses of which are the more important shutdown signals. The event-signal matrices established here provide a complete set of reactor shutdown signals for different events in every different plant condition. This is not done in the ordinary safety analyses, where the shutdown signal for a given event is always ambiguous. Therefore one may obtain a clear understanding of how the plant will behave and what the roles of the reactor shutdown signals are in shutting down the plant should an accidental event occur.

Although there are always uncertainties in the analyses, the shutdown signal importance rankings still provide valuable guidance for allocating the resources and adjusting the plants operational and maintenance requirements. for example, the Limiting Conditions for Operation specified in the Technical Specifications [16] for different reactor shutdown signals could be treated separately based upon their importance values. The surveillance frequencies, maintenance arrangements, and the schedules for component replacement for different reactor shutdown signals could also be adjusted based on their safety significance values. Even the instrumentation for a shutdown signal could be strengthen if its associated risk were found to be unacceptable.

In the case of the work reported here, for example, it is found that the OTDT-H-T reactor shutdown signal appears most frequently based upon the signal-event matrices. Especially when some of the control systems are disabled, the OTDT-H-T signal has a good chance to serve as the shutdown signal which actually shuts down the reactor. In this situation, we may want the allowed outage time (AOT) for this shutdown function to be more stringent than that for other shutdown signals. Similarly, the surveillance frequency and the maintenance schedule for the shutdown circuit of the OTDT-H-T signal could also be adjusted to be commensurate with its importance and therefore to enhance the plant safety.

4.3 The Validation of the Safety Injection Signal due to the Steam Line Pressure-Low Signal

The signal validation technique based upon system interactions proposed here may be applied in areas where the system interactions can be explicitly identified. The following discussion first depicts the Safety Injection (SI) system, then illustrates the unintended SI signal caused by the closure of a main steam isolation valve (MSIV), then finally describes the validation of the SI signal as an example of this application.

4.3.1 The Impact of an Unintended Safety Injection

A high pressure safety injection (or emergency core cooling) system is actuated in a loss of coolant accident or in a steam line break accident. During the safety injection process, the highly concentrated boric acid solution at ambient temperature is injected into the RCS in order to limit or prevent further core damage. The safety injection system is extremely important for reactor safety. However, if incorrectly actuated, it can cause a serious thermal shock in pipes and nozzles as a result of introducing the injected cold water into the high temperature fluid system. Furthermore, it would take a long time, typically one to three days, depend upon the core life, in order to dilute the injected highly concentrated boric acid to a level which would allow the plant to restartup, particularly when the reactor core is near to its end of life. When the reactor core is at its end of life, the boric acid concentration is much lower than that at the beginning of core life. Much more water is needed in order to dilute a given amount of boric acid at the end of core life than is at the beginning of core life. A large amount of waste will also be generated in the process of boric acid dilution. Storing and shipping this waste is also a burden for the plant. Therefore the impact of an unintended safety injection to a nuclear power plant is far more serious than that of an automatic reactor shutdown in many aspects. Thus, it can be valuable to avoid an unintended actuation of the safety injection system.

4.3.2 The Unintended Safety Injection due to a MSIV's Closure

Should the steam line break, the steam line pressure-low signal will initiate the closure of all the main steam isolation valves (MSIVs) in order to prevent uncontrolled blowdown of all steam generators. Nevertheless, the closure of a MSIV during normal power

operation will conversely generate the steam line pressure-low signal and initiate an unintended safety coolant injection, as explained below.

The steam pressure transmitters in a Westinghouse-PWR plant are typically located inside the steam tunnels, where it is possible for them to experience adverse environmental conditions during a steam line break accident. Therefore the sensed pressure is compensated by a typical lead/lag ratio of 50/5 in order to cope with the adverse environmental instrument uncertainties. This high lead/lag ratio circuit will extrapolate the sensed steam pressure variation and generate a steam pressure signal which is about equal to the expected pressure which would occur 45 seconds in advance of real time. When one of the MSIVs closes, the steam line upon which it is seated on is terminated, and the total steam flow to the main turbine is suddenly decreased. Sensing the plunge of the inlet steam flow, the turbine control system, trying to maintain the turbine power, will open all of the control valves to their maximum openings. If the reactor is operating above a certain power level, the opening of the turbine control valves decreases the steam line pressure in a manner essentially equivalent to that of a steam line break event. Since the steam pressure drops dramatically, the lead/lag compensation circuits, with the large lead/lag ratio of 50/5, enlarge the pressure drop by about 10 times of the actual pressure drop. This compensated pressure signal quickly reaches the steam line pressure-low setpoint, and thus, induces a safety injection signal. However, this SI is undesirable since the transient will soon be terminated by reactor shutdown on S/G-level-low low trip (S/G-L-LL-T) signal. The S/G-L-LL-T signal is generated when the steam generator upstream of the fail-closed MSIV encounters a water level shrinkage causing by the steam pressure increase after the MSIV's closure [28].

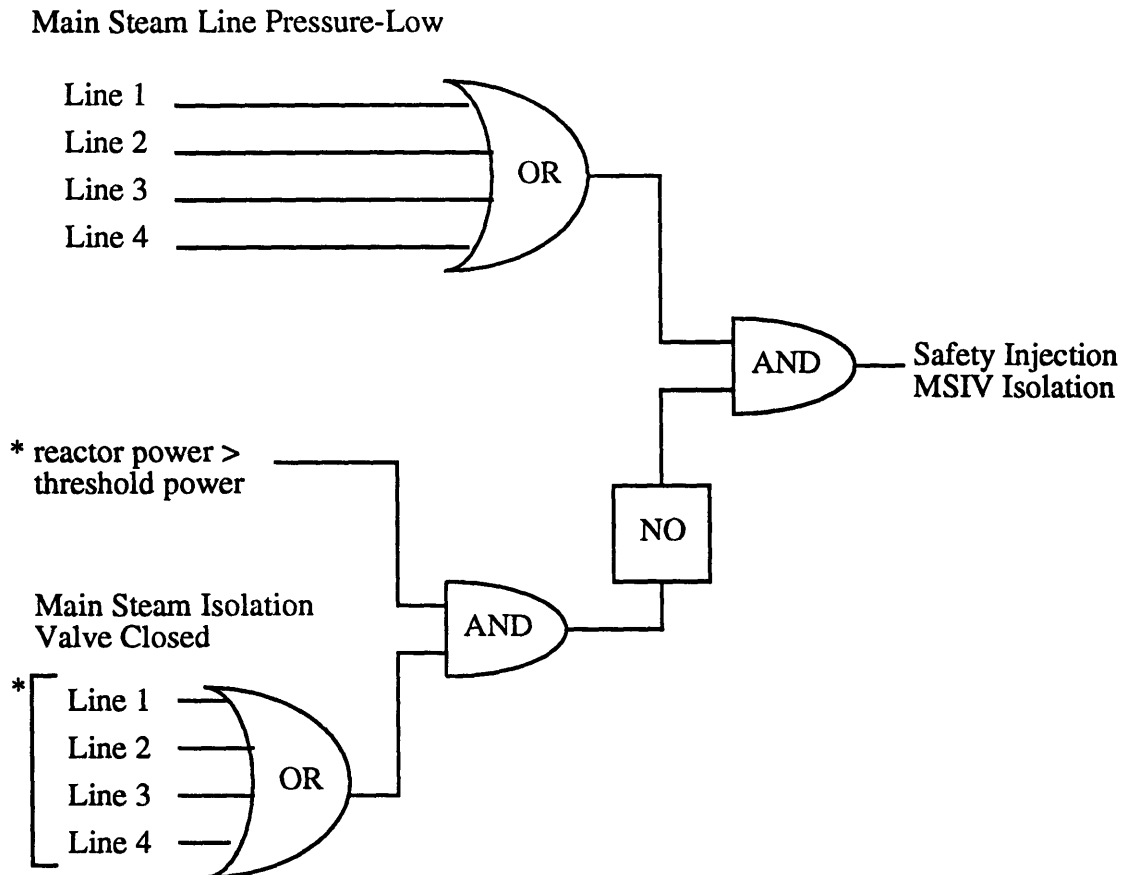
The MSIVs are designed to be fail-closed, and are located at the open space between the containment and the turbine building. The fail-closure of a MSIV is not unusual with the MSIV's being located in such adverse environmental conditions. Subsequently, the unintended safety coolant injection occurring due to the fail-closure of a MSIV is not unusual either. A nuclear power plant with a fail-closed MSIV will be automatically shut down as is discussed above. However, a safety coolant injection is not at all required, and is economically as well as technically harmful.

4.3.3 The Elimination of the Unintended Safety Injection

It is undesirable to generate the steam line pressure-low signal, which in turn will induce the SI signal, arising from the closure of a MSIV when the reactor power exceeds a certain "threshold" level . If it is the closure of the MSIV that generates the steam line pressure-low signal, then the MSIV-closure signal will precede the steam line pressure-low signal. If the steam line pressure-low signal is generated by a steam line break, then the MSIV-closure signal will lag behind the steam line pressure-low signal, since it is the steam line pressure-low signal that initiates the MSIV closure. Therefore we may use the MSIV closure signal as an interlock to validate the steam line pressure-low signal, and, in turn, the SI signal. This interlock permits the steam line pressure-low signal to actuate the SI signal only if no MSIV is closed previously and the reactor is operating above the threshold power level.

As is shown in Figure 4.3, the logic modification needed for eliminating the unintended SI caused by the closure of the MSIV is straightforward. Only two AND gates and one NO gate are added into the existing circuit. When the reactor is operating above the threshold power level and there is any one MSIV closed, the AND gate upstream the NO gate will send a positive signal to the NO gate. The NO gate then will send a negative signal to the downstream AND gate and prevent the steam line pressure-low signal from being forwarded to actuate SI and MSIV isolation. On the contrary, a positive signal from the NO gate means that all of the MSIVs are in open condition and the reactor is operating above the threshold power level, and therefore allows the steam line pressure-low to initiate the safety coolant injection. When the reactor is operating at a power level less than the threshold power, the NO gate will send a positive signal to the downstream AND gate. This simply resumes the function of the modified circuit back to that of the original circuit, and provides the SI and MSIV isolation functions for steam line break event when the reactor is operating at a low power level or is in hot stand-by condition.

The required circuit modification for SI signal validation is expected to be simple, effective and low-cost. It also prevents the unintended SI in an on-line fashion. Since not setpoint has been changed for the purposes of the SI signal validation, it is expected that the benefits from implementing the required circuit modification will outweigh the associated costs.



* Modified system input signals are asterisked.

Figure 4.3. The Logic Modification for Eliminating Unintended Safety Injection Due to MSIV's closure.

The NO gate is used to generated a negative output whenever there is any one MSIV closed before a SI signal is generated when the reactor is operating above the threshold power. This allows the elimination of the spurious SI signals arising from the MSIV's closures.

The NO gate generated a positive output in order to allow the Steam Line Pressure-Low signal actuating the safety coolant injection and MSIV isolation, if the SI signals are not caused by the MSIV's closures.

Chapter 5: Conclusions

5.1 Summary

In the work reported here, a Westinghouse 4-loop PWR is chosen for examination in order to demonstrate the concept of the reactor protection signal validation based on the effects of systems interactions. The systems interactions and the occurrence of signals during the postulated transients are simulated using the PRISM code. Based upon the simulations, a set of event-signal matrices corresponding to different plant conditions are constructed. From the constructed event-signal matrices, the signals that will lead a certain automatic reactor shutdown signal in appear in each anticipatory event are identified. These leading signals can be used to validate the reactor shutdown signals. The criteria set forth in this work for selecting the leading signals as the validation signal are as follows:

1. To avoid common cause failure, the validating signals and the shutdown signal to be validated can not share the same sensors or support systems.
2. Whenever there is a common signal leading different reactor shutdown signals in occurrence, it should be preferentially chosen for use in order to reduce the scale of circuit modifications as well as the subsequent operating costs.
3. The validating signals should survive any credible operation condition of the plant.

The validating-validated signal pairs selected according to these criteria are listed in Table 3.11. One of the merits of the RPS signal validation is that not any setpoint of the existing reactor protection as well as control systems is required to be changed.

Although some of the identified processes of shutdown signal validation may be dependent upon the reactor power level, the work reported here shows that only one set of signal validation circuits is adequate for use at any reactor power level. The RPS logic modification based upon the identified signal pairs is expected to be simple, reliable, low-cost. It provides an on-line means of prevention of unintended reactor shutdowns without any signal setpoint having to be changed.

The costs involved in the implementation of the proposed RPS modifications in a plant

is not expected to be too high as a result of the following two reasons:

1. Since not any signal setpoint in the existing systems has been changed in the development of the proposed circuit modifications, the results of the safety analyses remain unchanged for a plant which would implement the proposed RPS modification. No new safety issue is expected to be involved in order to implement the RPS circuit modifications. As one would expect, the licensing process for a design change without having the results of the safety analyses of the plant been changed is more promising than that with having the analysis results been changed.

2. If an accurate computer code is used to establish the required event-signal matrices, a reference plant can be chosen as the example upon which to focus all of the initial analyses. The other similarly designed plants can modify the analyses from the reference plant in order to fit their own specific designs. In fact, this is the typical practice used to eliminate the duplication of work and also duplicated cost among the members of different plant Owner's Groups. The design of the hardware modifications and the licensing of the proposed logic circuit changes can also be standardized in like manner, with the costs being shared by the joint members, if it is so desired.

The signal validation technique proposed here is estimated to be highly cost-effective, with a marginal economic benefit/cost ratio in the order of \$12 million/ 0.1 million for a plant with twenty more years to operate. In addition to the economic benefits, there are other benefits resulting from less thermal hydraulic impacts upon the plant, less challenges to the safety systems of the plant, less possible NRC investigations and the subsequent possible reactor shutdowns, etc.

The event-signal matrices established here provide an complete set of exact reactor shutdown signals for different events in every different plant condition. Therefore one may obtain a clear understanding in how the plant will behave and what are the roles of the reactor shutdown signals in shutting down the plant, should an event occur.

Other information drawn from the event-signal matrices is the importance ranking among the reactor shutdown signals. Although there are always uncertainties in the analyses, the shutdown signal importance rankings are still a good guidance for allocating the resources and adjusting the operation and maintenance requirements. The Limiting Conditions for Operation specified in the Technical Specifications for different reactor

shutdown signals could be treated separately based upon their importance. The surveillance frequencies, maintenance arrangements, and the schedules for component replacement for different reactor shutdown signals could also be adjusted based upon their safety significance values. The instrumentation for a shutdown signal could also be strengthened if the associated risk is found to be unacceptable.

The signal validation based upon system interactions is expected to be applicable in any areas where the system interactions can be explicitly identified. In the work described here, the validation of the safety injection signal arising from MSIV's closure is demonstrated as an example of the application.

5.2 Conclusions and Recommendations

The signal validation technique based upon system interactions is found to have the characteristics as follows:

1. It can prevent unintended incidents, such as spurious reactor shutdown, spurious safety coolant injection, from being occurred in an on-line fashion.
2. No setpoint in the plant has to be changed in order to employ the required RPS modification based upon this signal validation technique.
3. The results of the safety analyses remain unchanged, the safety licensing for the application of the technique is not expected to be difficult.
4. The required RPS circuit modification is expected to be simple, reliable, compatible to the existing systems, and having no adverse effect on the plants.

As a result of the above characteristics, the signal validation technique proposed here is estimated to be highly cost-effective, with a marginal economic benefit/cost ratio in the order of \$12 million/ 0.1 million for a plant with twenty more years to operate. In addition to the direct economic benefits, there are other benefits resulting from less thermal hydraulic impacts upon the plant, less challenges to the safety systems of the plant, and less possible NRC investigations and the subsequent plant shutdowns, etc.

Based upon the generally satisfactory results in signal validations as well as in operational improvements of the work reported here, it is recommended that the signal validation method based upon system interactions be further investigated by using more accurate computer codes, with the effects arising from the factors such as power level, core burn-up, plant specific setpoints, etc., should be incorporated into simulations.

References

- 1 Shih-Ping Kao, "PRISM: An Integrated RCS and Steam Generator Simulation Model," Presented at International Topical Meeting on Advances in Mathematics, Computations and Reactor Physics, Pittsburgh, PA, USA, April 1991.
- 2 "Nuclear Unit Operating Experience: 1985-1986 Update," EPRI NP-5544, Dec. 1987.
- 3 E. Michael Blake, "U.S. capacity factors: Soaring to new heights," Nuclear News, May 1993.
- 4 J. W. Cletcher, "Reactor Shutdown Experience," Nuclear Safety, 34, 1, Jan.-March 1993.
- 5 H. P. Polenta et al., "Implementation of a Fault Detection Procedure," Proc. 1986 American Control Conference, Seattle, Washington, USA, June 1986.
- 6 R. N. Clark and B. Campbell, "Instrument Fault Detection in a Pressurized Water Reactor," Nuclear Technology, 56, 23, 1982.
- 7 O. L. Deutsch et al., "Validation and Integration of Critical PWR Signals for Safety Parameter Display Systems," EPRI NP-4566, May 1986.
- 8 O. Glockler, B. R. Upadhyaya, and T. W. Kerlin, "Signal Validation Algorithms for Consistency Checking and Sequential Probability Ratio Testing of Redundant Measurements, DOE/NE/37956-6, U.S. Department of Energy, July 1987.
- 9 A. Descrochers and S. Mohseni, "On Determining the Structure of a Nonlinear System," Int. J. Control, 40, 5, 1984.
- 10 Z. Frei and B. R. Upadhyaya, "Empirical Modeling of Steady-State Behavior of Linear and Nonlinear Systems with Application to Signal Validation," DOE/NE/37959-11, U.S. Department of Energy, Aug. 1987.

- 11 B. R. Upadhyaya and K. E. Holbert, "Computation Data Driven Models with Application to Power Plant Signal Validation," Trans. Am. Nucl. Soc., 57, 276, 1988.
- 12 K. E. Holbert and B. R. Upadhyaya, "An Integrated Signal Validation System for Nuclear Power Plants," Nuclear Technology, 92, 3, Dec. 1990.
- 13 V. M. Morgenstern, B. R. Upadhyaya, and O. Glockler, "Signal Anomaly Detection and Characterization," DOE/NE/37959-18, U.S. Department of Energy, Aug. 1988.
- 14 W. Miller and J. Dayle, "Tennessee Valley Authority Becomes First to Install Digital Process Protection System," Nucl. Eng. Int., Feb. 1991.
- 15 "Systems Interaction Identification Procedures," EPRI NP-3834, July 1985.
- 16 "Standard Technical Specifications, Westinghouse Plants," NUREG 1431, NRC Sept. 1992.
- 17 "Precautions, Limitations, and Setpoints for Maanshan Nuclear Power Station," Rev 3, Taiwan Power Company, 1988.
- 18 "Final Safety Analysis Report--Maanshan Nuclear Power Station Unit 1 and Unit 2," Rev.15, Taiwan Power Company, May 1993.
- 19 J. R. Wang and S. F. Wang, "RETRAN02/MOD3 Analysis of Maanshan Unit 2 Start-up Tests," Proc. 3rd Int. Topical Meeting on Nuclear Power Plant Thermal Hydraulics and Operations, Seoul, Korea, Nov. 1988.
- 20 J. R. Wang and S. F. Wang, "Steam Generator Tube Rupture Analyses for Maanshan Using RETRAN-02/MOD3 Code," Proc. of the anticipated and Abnormal Transients in Nuclear Power Plants, Atlanta, Georgia, April 1987
- 21 J. R. Wang and S. F. Wang, "Analysis of Steam Line Break Accident for Maanshan Units 1 & 2 Using RETRAN-02/MOD2 Code," Proc. 2nd Int. Topical Meeting on Nuclear Power Plant Thermal Hydraulics and Operations, Tokyo, Japan, Apr. 1986.

- 22 S. F. Wang, J. R. Wang and J. R. Wang, "Steam Generator Tube Rupture Analyses for Maanshan Nuclear Power Plants," INER-0747, Dec. 1987.
- 23 J. R. Wang and S. F. Wang, "RETRAN02/MOD3 Analysis of the Maanshan Unit 2 Plant Trip from 100% Power," Trans. Am. Nucl. Soc., 56, 623, 1988.
- 24 J. R. Wang and S. F. Wang, "Nodalization Study of the Model F Steam Generator Secondary Side Using RETRAN-02/MOD3 Code," Trans. Am. Nucl. Soc., 56, 1988.
- 25 R. Y. Yuann, J. R. Tang, and S. F. Wang, "Boron Dilution Event Analysis for Maanshan Units 1 & 2 Using Hand Calculation Method and RETRAN-02 Code," Proc. 2nd Int. Topical Meeting on Nuclear Power Plant Thermal Hydraulics and Operations, Tokyo, Japan, Apr. 1986.
- 26 B. S. Pei, G. P. Yu, J. C. Kang, R. Y. Yuann, "Analysis of the Maanshan Unit 2 Turbine Trip Transient Using RELAP5/MOD2 and RETRAN-02/MOD2 Codes," Proc. 3rd Int. Topical Meeting on Nuclear Power Plant Thermal Hydraulics and Operations, Seoul, Korea, Nov. 1988.
- 27 R. Y. Yuann, S. C. Chiang, J. K. Hsius, P. C. Chen, "Safety Analysis for Turbine Trip Event with a Consequential Loss of Forced Reactor Coolant Flow," Proc. 3rd Int. Topical Meeting on Nuclear Power Plant Thermal Hydraulics and Operations, Seoul, Korea, Nov. 1988.
- 28 J. C. Kang and S. C. Chiang, "Feasibility Study on the Relaxation of the Secondary Side Safety Injection Setpoint Lead-Lag Ratio for Maanshan Nuclear Power Plant," Proc. 4th Int. Topical Meeting on Nuclear Power Plant Thermal Hydraulics and Operations, Taipei, Taiwan, Apr. 1994.
- 29 Shih-Ping Kao, "A Multiple-Loop Primary System Model for Pressurized Water Reactor Plant Sensor Validation," Ph. D. Thesis, Dept. of Nuclear Engineering, MIT, July 1984.
- 30 M. Massoud, Shih-Ping Kao, and N. Todreas, "Evaluation of Horizontal Steam Generator for PWR Application," MITNPI-TR-016, MIT, Aug. 1987

- 31 “ How Japanese Plants Reduce Their Trips,” WOG TRAP News, Westinghouse Electric Corporation, Summer 1991.
- 32 “ATWS Mitigation System Actuation Circuitry,” DCR-76085, Maanshan Nuclear Power Station Units 1 & 2, Taiwan Power Company, 1987.
- 33 “Project Description” Proceedings of October 1993 WOG general Session, Westinghouse Electric Corporation, Oct. 1993.