Reprinted from March 1983, Vol. 105, Journal of Dynamic Systems, Measurement, and Control

J. C. Deckert[1]

J. L. Fisher

D. B. Laning

A. Ray

The Charles Stark Draper Laboratory, Inc., Cambridge, Mass. 02139

Signal Validation for Nuclear Power Plants

A signal validation methodology to improve the reliability of the information displayed to the operator of a nuclear power plant is presented. The general design methodology is developed and then applied to the steam generator and feedwater subsystem of a typical pressurized water reactor. Using steady-state and transient simulations of this subsystem, including realistic additive sensor noise, the developed algorithm successfully isolates a variety of injected sensor faults and demonstrates its inherent capability to isolate common-mode sensor failures and plant component failures.

Introduction

Safety and reliability of complex processes such as those in a nuclear power plant are largely dependent upon the validity and accuracy of sensor signals that indicate plant operating conditions. Although many approaches to signal validation have been reported (e.g., reference [1]), current practice in nuclear power plants is restricted to a few rudimentary techniques such as like-sensor comparisons, limit checking, and auctioneering [2]. While such techniques generally serve to improve plant safety, limitations such as the inability to identify gradual drifts and insensitivity to common-mode failures[2] significantly curtail their effectiveness. These limitations can be circumvented by the application of advanced computerized diagnostic techniques related to those developed for aerospace systems. These techniques promise not only to aid plant operators in making proper and timely decisions, thereby enhancing plant safety, but also to improve plant availability.

The signal validation methodology adopted in this study demonstrates a systematic, unified approach to real-time detection and isolation of sensor and plant component failures by exploitation of available redundant information. Redundancy is classified as direct when two or more sensors are measuring a given plant variable, and analytic when an additional evaluation of a plant variable is analytically obtained from the physical relationships among various plant variables.

Unless three identical collocated sensors of a variable are available, some form of analytic redundancy, however elementary, must be employed to isolate the failure of one sensor of that variable. It is important to note that the developed approach recognizes the following inherent interrelationships between analytic redundancy and the reliable isolation of sensor failures and plant component failures: 1) analytic redundancy either explicitly or implicitly models the normal operation of one or more plant components; and 2) if the possibility of the failure of that component is not recognized at the outset and incorporated into the design, the failure of that plant component may be incorrectly interpreted as a sensor failure, with possibly far-reaching consequences.

In the remainder of the paper, we discuss the basic signal validation algorithm design methodology and the results of its application to the simulated steam generator and feedwater (SG/FW) subsystem of the secondary coolant system of a pressurized water reactor (PWR) power plant. A salient feature of the developed algorithm is the use of parity-space representation [3, 4, 5] to detect and isolate failures via the relative inconsistencies among all measurements, both direct and analytic. In contrast to many other approaches (e.g., reference [6]), this parity-space technique does not rely on detailed knowledge of sensor and plant noise statistics and failure modes, but instead uses readily available information on unfailed signal error magnitudes to define thresholds that are assumed to be exceeded only when failures are present. In addition, the developed methodology does not require banks of linearized differential equations (e.g., references [6, 7, 8]) that can become computationally burdensome and are particularly vulnerable to changes in the assumed plant dynamics, such as those arising from component failures.

Basic Design Methodology

Introduction. The signal validation and fault isolation philosophy embodied in this paper is that plant safety in general, and the operator's control and monitoring tasks in particular, are enhanced if critical plant component faults are isolated to the finest resolution practical in the shortest possible time. As discussed below, this seemingly self-evident notion forms the basis for a general design procedure that can be extremely useful in applying advanced fault isolation techniques, particularly analytic redundancy, to a specific plant and in tailoring the design to the user's unique needs.

Signal Validation Flow Diagram. The general structure of a signal validation algorithm is defined by a flow diagram

[1] Currently with ALPHATECH, Inc., Burlington, Mass. 01803.

[2] The failure of two or more elements in an identical manner, possibly due to a common cause.

Contributed by the Dynamic Systems and Control Division for publication in the JOURNAL OF DYNAMIC SYSTEMS, MEASUREMENT, AND CONTROL. Manuscript received by the Dynamic Systems and Control Division, September 30, 1981.

indicating the manner in which sensor output signals are combined to perform both fault isolation and parameter estimation. The flow diagram provides a pictorial summary of the utilization of sensor information, without the need to specify the details of the algorithm, by employing two generic building blocks: the analytic measurement calculator and the decision/estimator (D/E).

Each analytic measurement calculator uses an appropriate physical relationship, such as a conservation law or the normal operating characteristics of a hardware element, to combine signals representing estimates of unlike variables in such a way as to synthesize an indirect measurement of another variable. This analytic measurement may represent the only source of knowledge concerning that variable, or it may subsequently be compared with direct sensor measurements of the variable in a D/E to increase the reliability of the variable estimate and to aid in fault detection and isolation.

Each D/E has as its inputs all of the direct and analytic measurements of a single variable of interest. The D/E forms a "validated" estimate of the measured variable using a consistent subset of its input measurements, and it employs measurement inconsistency information to determine when one or more of its input measurements has failed. The transfer of this failed measurement information to the plant operator is the most important task of the algorithm.

The generic nature of these building blocks affords the designer a great deal of flexibility. He can choose the physical relationships used by the analytic measurement calculators as well as the methods employed to determine measurement consistency and to calculate variable estimates within the D/Es. Having recognized the latitude available to the designer, the general procedure for signal validation flow diagram design is now introduced with a discussion of the effect of diagram architecture on fault isolation resolution.

Fault Isolation and Least Plant Units. In order to infer component failures from measurement inconsistencies detected by a D/E, it is useful to introduce the concept of a least plant unit (LPU). When more than two input measurements are available to a D/E, there is an LPU associated with each measurement, defined as the aggregate of all those physical components whose individual failures could cause that measurement to be inconsistent with the other input measurements. When there are only two input measurements to a D/E, there is a single similarly-defined LPU associated with both input measurements. Thus LPU size reflects the fault resolution capability of the signal validation algorithm, and the desire to achieve fine fault-isolation resolution implies that LPU size must be kept small.

Because the LPU associated with a direct sensor measurement is the sensor itself, its size is fixed. However, the size of an analytic measurement's LPU is strongly affected by flow diagram architecture. In particular, LPU size will be smallest when the number of unvalidated estimates (i.e., single sensor outputs) used in the analytic relationship is minimized. Therefore, minimized use of unvalidated estimates in analytic relationships is a flow diagram design guideline. Because every analytic measurement calculator either explicitly or implicitly models the normal operation of some plant component, each analytic measurement LPU contains at least one plant component; it is through this mechanism that plant component failures can be isolated.

Although the LPU represents basic fault isolation resolution, fault isolation to a level within an LPU is possible by logical inference when the same physical element belongs to more than one LPU. To illustrate this, consider the case of one LPU composed of the elements A, B, and C, and another LPU composed of the elements C, D, and E. If at nearly the same time these two LPUs fail, i.e., if their associated analytic measurements are found to be inconsistent, then it is likely that their common element, element C, is faulty. Conversely, if the first LPU fails but the second LPU does not, it is likely that their common element is not faulty and that instead either element A or element B has failed.

It is important to emphasize that the above reasoning for LPU and sub-LPU fault isolation relies on the assumption that single element failure is the dominant mode, a good assumption for a properly designed system. However, regardless of the particular failure probability assumptions used by a D/E in declaring element failures, other less likely explanations for the observed measurement inconsistencies should also be displayed to the operator.

Flow Diagram Design Procedure. The design of a signal validation flow diagram is an iterative process. Its natural starting point is the establishment of the critical functions within the subsystem of interest to be supported by the design. These functions could be mathematical functions or operator tasks, but in either case they require the validated estimates of certain key variables whose importance dictates that most, if not all, of them will be measured directly. The design of the signal validation flow diagram therefore begins with the provision of a D/E for each key variable, with a validated estimate as output and every direct measurement as an input.

The next step in the design process involves an assessment of the adequacy of the direct measurement redundancy for each critical variable. At least two measurements are required to allow the formation of a validated estimate, and at least three measurements are required to allow a valid estimate to be formed following a single sensor failure. Therefore, because of the critical nature of these key variables, the design process continues via addition of either direct measurements (i.e., more sensors) or analytic measurements as inputs to those D/Es with fewer than three inputs until the desired level of redundancy is reached.

Because the addition of more sensor hardware is often not feasible, analytic measurements may be the only source of supplemental redundancy. As mentioned above, the guideline that applies in this case is to minimize the number of unvalidated estimates used for each analytic redundancy relationship. The benefits of analytic redundancy, i.e., its ability to isolate common-mode sensor failures and plant component failures and the supplementary redundancy it adds to the sensor complement, must be weighed against the realization that for actual, nonidealized systems the error in an analytic measurement is often higher than that in a direct measurement.

Initially, the types of analytic relationships to be used to generate analytic measurements of a variable should be limited only by the unavailability of (direct or analytic) measurements of required variables. It is important to note that a measurement of any quality (e.g., worst-case error with unfailed inputs, or noise standard deviation) can be used for fault detection and variable estimation as long as its D/E threshold reflects that quality. For example, if every threshold for a D/E is equally proportional to the standard deviation of its input measurement noise, then the minimum variance estimate of the measured variable can be calculated as the weighted average of the consistent measurements, where the individual weights are inversely proportional to the square of the respective thresholds [4].

At this stage, iteration on the design can be prompted by a variety of reasons including: impracticality of the addition of sensors to achieve the desired level of redundancy; deficiency in the number of available independent analytic relationships; relatively high noise, bias, or modeling complexity for some available analytic relationships; the desire to isolate sufficiently probable common-mode sensor failures or com-

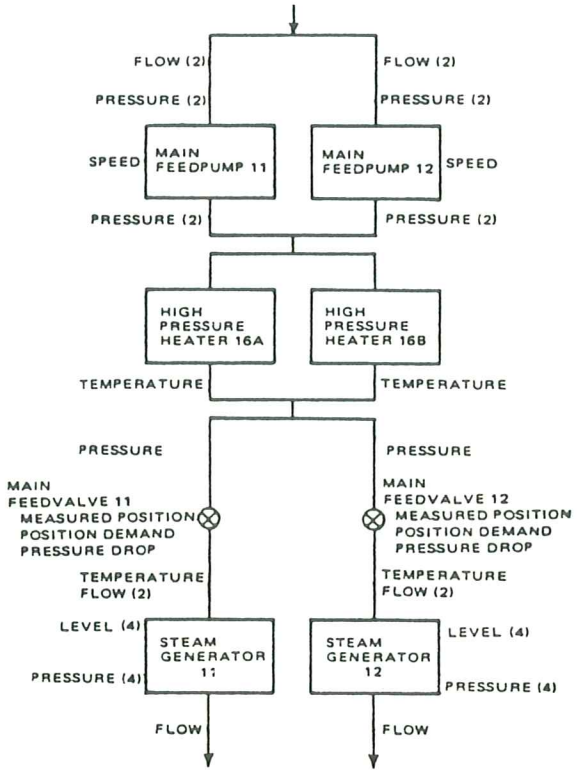

Fig. 1 Steam generator and feedwater subsystem measurements

ponent failures; the need for additional redundancy suggested by likely degraded sensor configurations; or the desire to decrease the size of a particular LPU.

The final signal validation flow diagram resulting from this iterative process in most cases will represent a compromise between hardware complexity in the form of sensor redundancy and software complexity in the form of analytic redundancy and D/E computations. The use of available a priori component failure probabilities can be useful in assessing candidate designs in terms of the probability of erroneous estimates of the critical variables. A reasonable groundrule in the absence of sufficient a priori statistics is that no single element failure should result in an erroneous estimate's use in critical functions.

Application to the Steam Generator and Feedwater Subsystem

Introduction. The SG/FW subsystem of a typical PWR was chosen for study because utility experience has shown that its improvement can contribute substantially to overall plant availability [9]. Figure 1 illustrates the layout of the plant components and sensors of the reference subsystem, with sensor replication noted in parentheses. The scope of the study included all the major plant components and sensors located between the low pressure heaters and the turbine-generator system, with the developed algorithm performing signal validation on a total of forty-eight sensors and ten plant components in two parallel legs.

In order to demonstrate the power of the technique, the signal validation flow diagram was designed to isolate a failed sensor to the sensor level wherever possible. This was accomplished for all sensors except a failed feedpump speed sensor, which can only be isolated to the level of feedpump speed sensor and feedpump, and a failed steam flow sensor, which can only be isolated to the level of steam flow sensor and steam generator.

Figure 2 illustrates the signal validation flow diagram developed for the reference SG/FW subsystem, with the symmetric structure for the second leg omitted for clarity. Each analytic measurement calculator is shown as a logical "AND" gate, suggested by the fact that the validity of its output requires validity of all its inputs; while each D/E is shown as a logical "OR" gate, suggested by the fact that its output estimate can be good even if some of its input measurements are faulty. The arrow emerging obliquely from each D/E is used to indicate the input measurement consistency or failure information being collected. Direct sensor measurements are enclosed in ovals; the steam generator heat rate input from the primary coolant loop, assumed validated elsewhere, is enclosed in a rectangle.

Design Details. In this study, each D/E determines input measurement consistency using a parity-space algorithm employing an identical threshold for all direct and analytic input measurements [10]. (Recall that this algorithm has been extended to employ a different threshold for each D/E measurement [4, 5].) Every second the validated output estimate is formed as the average of the consistent input measurements, where inconsistent measurements are determined on the basis of the magnitude and direction of the parity vector. LPU failures are declared using a multiple-consecutive-miscomparison (MCM) criterion: if a measurement is found to be inconsistent on N consecutive samples, that measurement is eliminated from future consideration and its LPU is declared to be failed. Although suboptimal, the MCM criterion using an ad hoc choice for N of 3 performed well in this study.[3] Therefore, more elaborate fault declaration techniques, requiring accurate (and usually scarce) sensor noise models for optimality, were not deemed necessary.

Five simple explicit models of plant components are used in the analytic measurement calculators in Fig. 2: the main feedvalve stroking mechanism; the main feedvalve flow/pressure-drop characteristics; the high pressure heater flow/pressure-drop characteristics; the main feedpump similarity relationship; and the steam generator steam flow as a function of steam generator liquid level and pressure, feedwater flow and temperature, and input power. The main feedvalve stroking mechanism response to demand changes is modeled as constant speed, with 15 seconds required to move between fully-opened and fully-closed positions. The main feedvalve effective area is modeled as a quadratic function of stem position. From steady-state conservation of momentum, feedwater flow is modeled proportional to the effective valve area times the square root of the pressure drop across the valve, and the pressure drop through the two high pressure heaters is modeled as a constant times the square of the total feedwater flow. The main feedpump is modeled as a piecewise quadratic function relating (head ÷ pump speed^2) to (feedwater flow ÷ pump speed). The steam generator steam flow model, using conservation of mass and energy, contains no differential equations except for first-order filters on feedwater flow and steam generator drum pressure; it requires only thirty-four multiplications and thirty-two additions.

Fault Isolation Examples. As mentioned above, the flow diagram shown in Figure 2 was designed primarily to isolate the first failure of any sensor. To illustrate how this isolation is done, the technique will be described for feedwater flow and steam generator pressure measurements.

A validated estimate of the feedwater flow into each steam

[3] A better choice of N can be obtained by optimizing the tradeoff between false alarms and detection delay for assumed measurement noise probability densities [10].

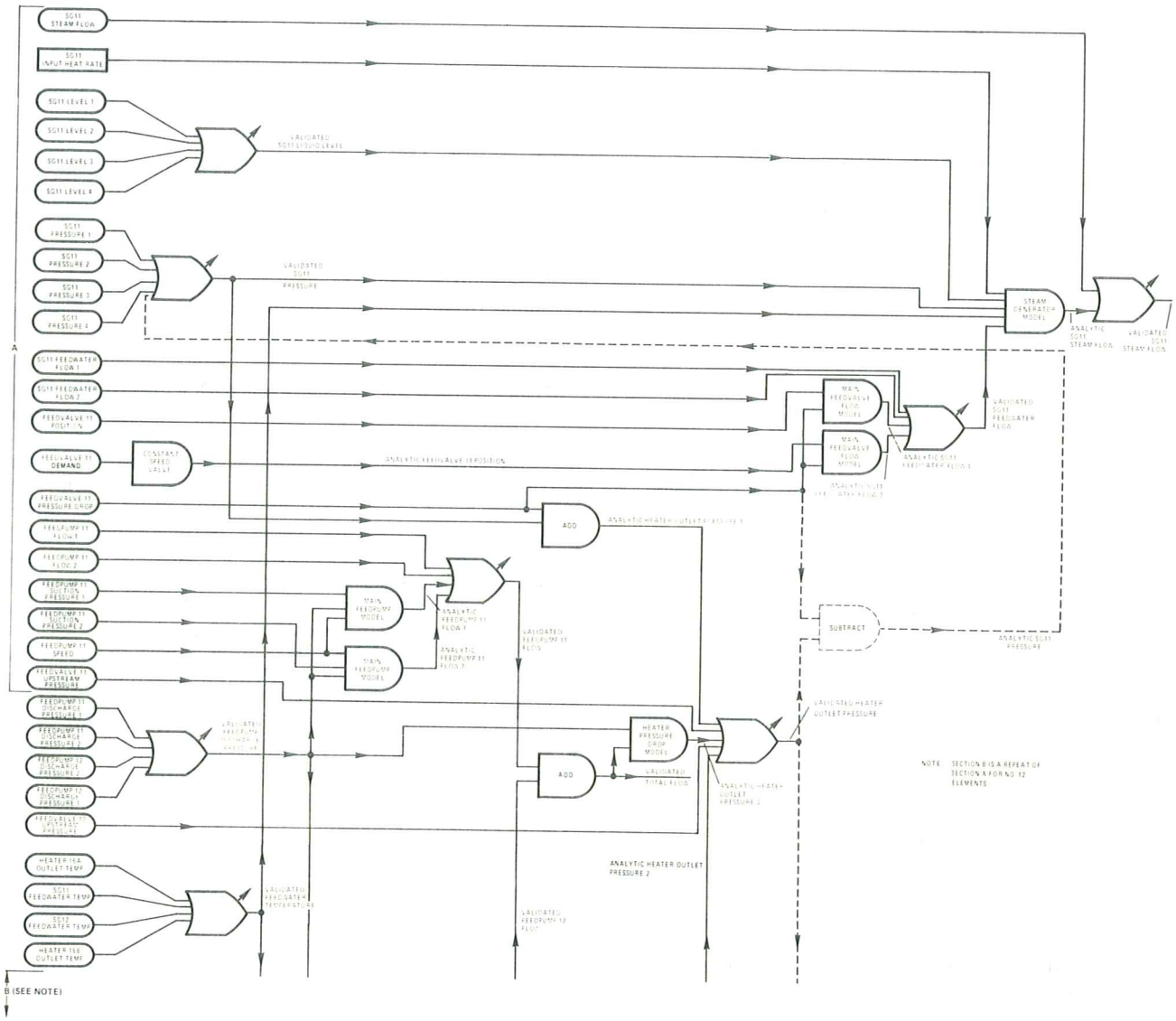

Fig. 2 Signal validation flow diagram

generator is obtained by a D/E with two direct and two analytic measurement inputs. Each analytic measurement calculator uses the same main feedvalve flow model and differential pressure sensor, with one utilizing the direct feedvalve stem position measurement and the other using an analytic measurement calculated using the demand signal through the constant-speed stroking mechanism model. Assuming that the feedvalve position demand signal is always accurately known, the four LPUs associated with this D/E are: 1) feedwater flow sensor 1; 2) feedwater flow sensor 2; 3) feedvalve position sensor, feedvalve differential pressure sensor, and feedvalve; and 4) feedvalve stroking mechanism, feedvalve differential pressure sensor, and feedvalve.

The failure of either feedwater flow sensor is easily isolated when one direct measurement is inconsistent with the other three measurements. The persistent inconsistency of one analytic measurement with the other three measurements is interpreted as the failure of that element within its LPU not common to the LPU for the other analytic measurement, i.e., either the feedvalve position sensor in the case of the inconsistency of LPU3 or the feedvalve stroking mechanism in the case of the inconsistency of LPU4. Assuming that single element failures are more probable than common-mode failures, either the quickly successive failure of the two analytic measurements or the simultaneous pairwise grouping of the two direct and two analytic measurements is interpreted as the failure of one of the elements common to both analytic measurement LPUs (LPU3 and LPU4), i.e., the differential pressure sensor or the feedvalve itself. Also note in Fig. 2 that a sufficiently large failure of the differential pressure sensor will result in the miscomparison of its associated analytic heater outlet pressure measurement with the other four measurements.

Table 1 Bias failure summary

SENSOR TYPE	UNITS	NORMAL ERROR (NOISE)	ERROR THRESHOLD	100% POWER		50% POWER	
				NOMINAL VALUE	BIAS FAILURE	NOMINAL VALUE	BIAS FAILURE
FEEDPUMP SUCTION PRESSURE	kPa (PSI)	±35 (±5)	†	3965 (575)	±414 (±60)	5102 (740)	±138 (±20)
FEEDPUMP OUTLET PRESSURE	kPa (PSI)	±75 (±11)	83 (12)	7722 (1120)	±207 (±30)	6895 (1000)	±207 (±30)
FEEDPUMP FLOW	kg/s (LB/HR)	±12.6 (±100,000)	50 (400,000)	796 (6,320,000)	±113 (±900,000)	360 (2,880,000)	±126 (±1,000,000)
FEEDWATER TEMPERATURE	°C (°F)	±1 (±2)	1 (2)	229 (445)	±3.3 (±6)	191 (376)	±3.3 (±6)
FEEDPUMP SPEED	rpm	±40	†	3900	±150	2530	±120
STEAM GENERATOR PRESSURE	kPa (PSI)	±62 (±9)	69 (10)	6205 (900)	±172 (±25)	6400 (926)	±172 (±25)
STEAM GENERATOR LEVEL	%	±2.5	2.5	70	±7	70	±7
FEEDWATER CONTROL VALVE DEMAND	%	±2	†	74	±8	43	±11
FEEDWATER CONTROL VALVE POSITION	%	±2	†	74	±9	43	±10
FEEDWATER CONTROL VALVE PRESSURE DROP	kPa (PSI)	±14 (±2)	†	241 (35)	±55 (±8)	117 (17)	±55 (±8)
FEEDWATER FLOW	kg/s (LB/HR)	±12.6 (±100,000)	28 (220,000)	796 (6,320,000)	±69 (±550,000)	360 (2,880,000)	±69 (±550,000)
STEAM FLOW	kg/s (LB/HR)	±12.6 (±100,000)	31.5 (250,000)	796 (6,320,000)	±75 (±600,000)	360 (2,880,000)	±75 (±600,000)
HIGH PRESSURE HEATER OUTLET PRESSURE	kPa (PSI)	±76 (±11)	103 (15)	6450 (935)	±310 (±45)	6516 (945)	±310 (±45)

† NO PARITY SPACE TEST IS PERFORMED ON THIS SENSOR; IT IS USED ONLY AS AN INPUT TO AN ANALYTIC MODEL

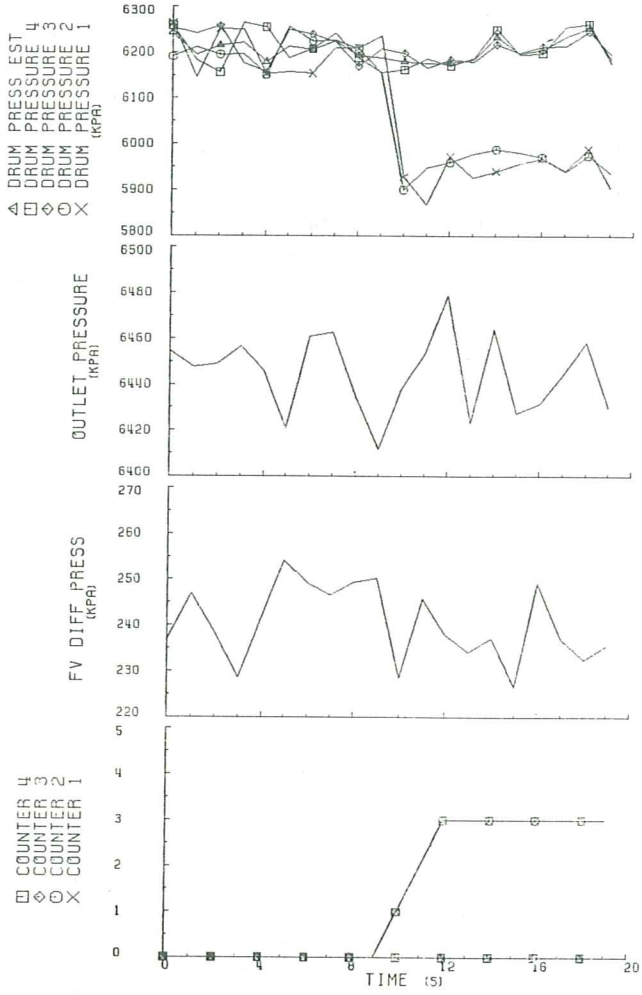

Fig. 3 Common-mode failure of two steam generator pressure sensors

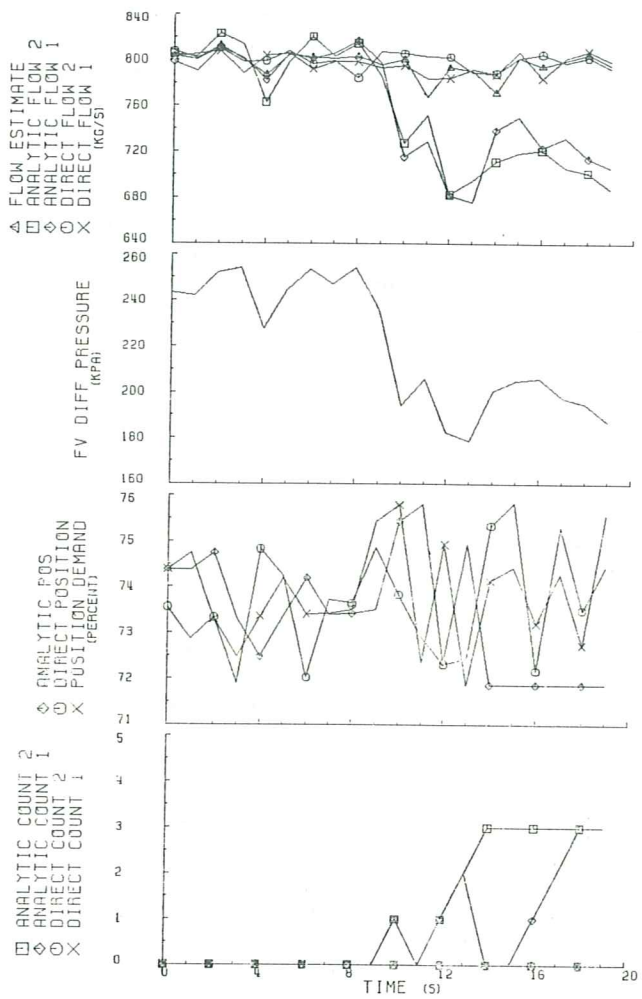

Fig. 4 Failure of main feedvalve differential pressure sensor

Steam generator drum pressure represents the one variable in Fig. 2 where sufficient redundancy exists to reliably isolate the common-mode failure of two of the four sensors in addition to single sensor failures. Whenever pairwise grouping of the four pressure sensor readings is observed, it is assumed that a common-mode failure has occurred. The difference between the unfailed feedvalve differential pressure measurement and the validated heater outlet pressure estimate is used as a supplemental analytic measurement to break the tie. This tie-breaker signal is shown in dotted lines in Fig. 2; it is not normally used because its noise is high relative to unfailed drum pressure sensor noise. It is important to note that the effect of steam generator input nozzle pressure drop could easily be incorporated using the validated estimate of feedwater flow.

Simulation Results. The Combustion Engineering, Inc., (C-E) ZAMBO3 feedwater system analytical design code was used to calculate accurate test cases [10]. The characteristics of Arkansas Nuclear One Unit 2 were chosen as the reference, and test cases for this reference plant were chosen so as to be representative of the SG/FW subsystem's behavior during steady-state and transient conditions, including step changes in turbine power, ramped loss of feedwater, and ramped increase in feedwater. During the evaluation of the signal validation technique, the SG/FW subsystem variables were corrupted with typical uniformly distributed sensor noise to simulate sensor outputs.

A variety of computer runs were made to verify and evaluate the signal validation program. All steady-state and transient ZAMBO3 test cases were run without simulated failures to verify that no false alarms occurred for the error thresholds used. Then positive and negative biases were systematically introduced into every sensor type at steady-state power levels. Table 1 shows the bias failure levels that were consistently identified at 100 and 50 percent steady-state power levels, together with the simulated uniformly distributed sensor error bounds and the D/E thresholds used. In each case identification was made within ten seconds of the failure onset. In general, the error size that could be identified was two to three times the threshold. It should also be noted that because the fault isolation techniques used in this study rely on robust modeling of plant processes, equivalent performance of the fault detection and identification algorithms is expected following introduction of failures during transients. This peformance was observed in several test runs using available ZAMBO3 transient data.

As described above and illustrated in Fig. 3, sufficient redundancy exists to isolate the common-mode failure of two drum pressure sensors in one steam generator. The first frame depicts the four steam generator drum pressure measurements and the drum pressure estimate. The second and third frames depict the high pressure heater outlet pressure estimate and the feedvalve differential pressure measurement, respectively. The fourth frame depicts the MCM counters, denoting the number of consecutive miscomparisons, for each of the steam

generator pressure measurements. The reactor is initially operating normally at 100 percent power. At 10 seconds pressure sensors 1 and 2 fail low. The failed pair is isolated by comparison with the outlet pressure estimate minus the differential pressure measurement. As a result, the only MCM counters that are incremented are those of the failed sensors, under conditions in which the parity-space algorithm based on only four measurements would have to count all sensors as failed. The figure also illustrates the fact that the estimate uses only the unsuspected sensor information during the period before the failed sensors are declared to be bad.

As previously discussed, a multiple-measurement failure can occur to the signal validation algorithm when one unvalidated sensor output is used as an input to more than one analytic measurement. Figure 4 illustrates the failure of the single differential pressure sensor for the feedwater control valve, which is used with two different measurements of valve position to create two analytic measurements of feedwater flow. The first frame depicts the two direct measurements of feedwater flow, the two analytic measurements of feedwater flow, and the feedwater flow estimate. The second frame depicts the differential pressure measurement. The third frame depicts the direct feedvalve stem position measurement, the feedvalve stem position demand signal, and the analytic feedvalve stem position measurement computed from the demand signal. The fourth frame depicts the MCM counters for the two direct and two analytic feedwater flow measurements.

At 10 seconds a bias failure of the differential pressure sensor occurs. The parity-space algorithm alone cannot determine the failed feedwater flow measurements since there are only four measurements, with two pairs of measurements agreeing internally. However, recognizing that the only single-point failure producing this situation affects the analytic flow calculations, the logic employed in this case deletes the two analytic measurements of feedwater flow from the final estimate if they differ from the two direct measurements in a similar way, i.e., both high or both low. This process occurs at 10, 12, and 13 seconds. The presence of noise causes recognition of failure of the two analytic measurements to occur at different times, at 14 and 18 seconds. The close time proximity of the failures of two LPUs involving common elements makes it easy to conclude that one of the common elements, the differential pressure sensor or the feedvalve itself, has in fact failed. Note that a similar pattern of LPU failures would have resulted if the feedvalve stem position/effective area relationship had changed.

Conclusions and Recommendations

The signal validation algorithm isolated relatively small sensor failures in steady-state and transient simulations in the presence of realistic additive sensor noise. Where more than three direct measurements were available, a sensor failure three times the magnitude of the uniform sensor noise was consistently isolated. Performance in identifying sensor failures via analytic redundancy varied from the ability to isolate a failure 3 percent of the nominal value of the feed-pump suction pressure sensor to the inability to isolate a failure smaller than 47 percent of the nominal value of the feedvalve differential pressure sensor, both at 50 percent plant power. (It is anticipated that the use of the multiple-threshold parity test, with the possibility of varying analytic measurement thresholds with plant state, would significantly improve the latter performance.) Additionally, the test results demonstrated the algorithm's ability to isolate common-mode sensor failures and plant component failures.

The nature of the signal validation methodology is to form validated variable estimates from redundant measurements, including analytic measurements formed using validated estimates wherever possible. The methodology allows the use of low dimension nonlinear models, which are robust over a wide range of operating conditions. This basic structure lends itself to a distributed processor implementation with a relatively small shared data base. Therefore the extensions of the methodology to the real-time monitoring of the complete PWR system or of other complex processes, such as fossil power plants and chemical plants, appears feasible.

Because this study has achieved the objective of demonstrating the potential for improved reliability of the information displayed to the operator of a nuclear power plant through the use of advanced fault isolation techniques, the recommended next step is a proof-of-principle demonstration using actual plant sensor data to include factors such as sensor dynamics, calibration errors, and physical separation; transport delays; and equipment variability. Although it is felt that these factors present no significant challenges to the developed signal validation approach, such a demonstration is mandatory in order for the approach to merit nuclear industry acceptance.

Acknowledgments

The work reported in this paper was sponsored by the Electric Power Research Institute through Combustion Engineering, Inc., Contract 11680. The authors gratefully acknowledge the data and technical insights provided by various C-E personnel, including C. T. French, J. N. Lanzalotta, C. H. Meijer, J. P. Pasquenza, and F. J. Safryn; and the contributions of their Draper Laboratory colleagues, M. N. Desai and J. J. Deyst.

References

1 Willsky, A. S., "A Survey of Design Methods for Failure Detection in Dynamic Systems," *Automatica*, Vol. 12, Nov. 1976, pp. 601-611.

2 Deyst, J. J., Kanazawa, R. M., and Pasquenza, J. P., "Sensor Validation: A Method to Enhance the Quality of the Man/Machine Interface in Nuclear Power Stations," IEEE Nuclear Power Symposium, Orlando, Florida, Nov. 5-7, 1980.

3 Potter, J. E., and Suman, M. C., "Thresholdless Redundancy Management with Arrays of Skewed Instruments," *Integrity in Electronic Flight Control Systems*, NATO AGARDograph-224, 1977, pp. 1-15 to 15-25.

4 Ray, A., Desai, M., and Deyst, J., "Fault Detection and Isolation in a Nuclear Reactor," *AIAA Journal of Energy*, Jan./Feb. 1983, pp. 79-85.

5 Desai, M., and Ray, A., "A Fault Detection and Isolation Methodology," Proceedings of the 20th IEEE Conference on Decision and Control, San Diego, California, Dec. 1981, pp. 1363-1369.

6 Tylee, J. L., "A Generalized Likelihood Approach to Detecting and Identifying Failures in Pressurizer Instrumentation," *Nucl. Technol.*, Vol. 56, Mar. 1982, pp. 484-492.

7 Clark, R. N., and Campbell, B., "Instrument Fault Detection in a Pressurized Water Reactor Pressurizer," *Nucl. Technol.*, Vol. 56, Jan. 1982, pp. 23-32.

8 Kitamura, M., "Detection of Sensor Failures in Nuclear Plants Using Analytic Redundancy," *Trans. Am. Nucl. Soc.*, Vol. 34, 1980, pp. 581-583.

9 Meijer, C. H., and Frogner, B. J., *On-Line Power Plant Alarm and Disturbance Analysis System*, Report NP-1379, Electric Power Research Institute, Palo Alto, Calif., Apr. 1980.

10 Meijer, C. H., et al., *On-Line Power Plant Signal Validation Technique Utilizing Parity-Space Representation and Analytic Redundancy*, Report NP-2110, Electric Power Research Institute, Palo Alto, California, Nov. 1981.