Reprinted from September 1986, Vol. 108, Journal of Dynamic Systems, Measurement, and Control

A Redundancy Management Procedure for Fault Detection and Isolation

Asok Ray
Department of Mechanical Engineering,
The Pennsylvania State University,
University Park, PA 16802
Mem. ASME

Mukund Desai
The Charles Stark Draper Laboratory,
Cambridge, MA 02139

This paper presents the theoretical basis of a novel redundancy management procedure developed for fault detection and isolation (FDI) in strategic processes such as spacecraft, aircraft, and nuclear plants where multiply-redundant measurements are available for individual variables. The set of redundant measurements may comprise both direct sensor outputs and analytically derived measurements. The redundancy management procedure presented in this paper is essentially independent of the fault detection strategy and measurement noise statistics, and builds upon the concept of partitioning the set of measurements into "consistent" and "inconsistent" subsets for purposes of estimation and fault isolation, respectively. The proposed procedure is suitable for real-time applications using commercially available microcomputers and its efficacy has been verified on-line in operating nuclear reactors.

1 Introduction

Safety, reliability, and performance of complex processes such as spacecraft, aircraft, and nuclear plants can be improved by utilizing systematic failure detection procedures [1–13]. The redundant measurements that are usually available for individual critical process variables comprise sensor outputs (possibly of different accuracies) in conjunction with analytically derived measurement(s) of the given variable. The analytic measurements are synthesized from physical relationships between measurements of other process variables as well as from known characteristics of the process itself [3, 9 10, 11]. In contrast to the state variable-based models of physical processes that are often employed to construct filters for fault detection [7, 8], analytic redundancy could be primarily used to resolve common-mode failures as well as to detect (non-sensor-related) plant component failures [9–11]. In that case, modelling errors and uncertainties incurred in analytic measurements have a relatively less significant bearing on the efficacy of accurate fault detection. This approach serves as a failure detection recourse where development of process models that are of appropriate accuracy and complexity for filter construction is not feasible.

Some of the better known existing fault detection procedures discussed in [1, 2, 7, 8, 9] are based on assumptions such as knowledge of the probability density function (or its characteristics) for both nominal and failed conditions, and existence of a well-defined process model that can be used for constructing a filter. For many industrial applications, measurement noise statistics are not completely known nor do they follow a specific pattern such as having a Gaussian distribution, and the available process models may be too complex or have insufficient accuracy to be used in the construction of a filter. In the absence of relevant statistical information, the noise model may be approximated as being amplitude-limited [10, 11, 14]. In that case, the maximum noise amplitude that does not exceed a specified error bound is interpreted to be acceptable under nominal operating conditions. The information on sensor and plant equipment that is routinely available from the manufacturers is usually sufficient to quantify such error bounds. However, if appropriate information on noise statistics is available, the aforementioned restriction can be lifted by assigning fixed probabilities for the noise amplitude being within the error bound for nominal and failed conditions, respectively. This can be accomplished by applying established procedures such as sequential tests of Wald [15], Shiryayev [16], and Chien [17] (for example see [18, 19]).

We propose a fault detection technique based on the aforementioned approach of requiring multiply-redundant measurements of a process variable along with a priori specified error bounds for each measurement. The latter requirement pertains to the assumption of having amplitude-limited noise and may be modified to accommodate additional noise statistics if they become available. The goal of this paper is to present the theory and application of a novel redundancy management procedure from both an algebraic and a geometric point of view, so that it can be used in the development of a fault detection and isolation methodology. The proposed redundancy management procedure makes use of all available measurements – sensor outputs and analytic redundancy – and is essentially independent of the failure detection strategy, the measurement noise statistics, and the associated assumptions such as amplitude-limited noise. An outline of the redundancy management procedure is provided below.

Contributed by the Dynamic System and Control Division for publication in the JOURNAL OF DYNAMIC SYSTEMS, MEASUREMENT, AND CONTROL. Manuscript received at ASME Headquarters, June 23, 1986.

Failure decisions should be made by concurrent checking of the "consistency" or "inconsistency" of the redundant measurements at each sample time. (Precise definitions of the terms in quotations and their physical interpretation are provided in Section 2.) Checking the consistency or inconsistency of each redundant measurement can be carried out by one of the following two options: (1) use of allowable error bounds associated with each measurement, where such bounds are specified a priori and may be time-varying; (2) use of the noise statistics of individual measurements provided that the available information is adequate for the development of a decision algorithm such as generalized likelihood ratio test [1, 2]. These options can be implemented either using single sample tests or via sequential tests based on the time history of both current and past observations. Use of both fixed and variable sample approaches may be appropriate for the above option #2 as reported earlier in [11, 18]. The variable sample approach could provide an optimal decision rule by minimizing a composite cost function consisting of the weighted sum of two opposing requirements such as the probability of false alarm adjoined with the time delay incurred in detecting the fault [15–17]. The fixed sample approach is usually computationally simpler although not necessarily optimal.

The redundancy management procedure presented in this paper can be used in conjunction with a fixed sample approach or a variable sample approach and is applicable to multiply-redundant systems where the measurements may be vector quantities (such as the velocity or acceleration of an object in space) or scalar quantities (such as the thermal power or coolant temperature of a nuclear reactor). For scalar measurements in particular, the redundancy management algorithm outlined in the paper does not require any multiplications and is, therefore, computationally fast and apparently suitable for real-time applications using commercially available microcomputers.

The paper is organized in several sections and Appendices. Section 2 discusses the theoretical development of the redundancy management procedure, its physical interpretation, and how to apply this procedure. Section 3 addresses the real-time aspects in applying this approach and experimental verification of this procedure to nuclear power plants while Section 4 contains the summary and conclusions. The supporting theorems, the geometric interpretation, and a sketch of a real-time algorithm (applicable for scalar measurements only) are given as Appendices A, B, and C, respectively.

Theory of the Redundancy Management Procedure

The (possibly time-varying) redundant measurements of a plant variable are modelled at the sample time t as

$$z(t) = [H(t) + \Delta H(t)]x(t) + \beta(t) + e(t) \tag{1}$$

where

z is an $(l \times 1)$ vector of available known sensor or analytic measurements,
H is an $(l \times n)$ a priori known measurement matrix of rank n; $l > n$,
ΔH is an $(l \times n)$ matrix representing unknown scale factor errors,
x is the $(n \times 1)$ unknown vector variable that is to be estimated,
β is an $(l \times 1)$ unknown vector of bias errors, and
e is an $(l \times 1)$ vector of measurement noises with $E(e) = 0$.

It is important to note that the dimension l of the measurement vector z must exceed the dimension n of the unknown vector variable x in order to be able to apply this technique.

In a recent publication [20] we have reported the development of a calibration and estimation filter where the combined effect of (nonlinear) scale factor and bias errors are represented as $c(t) = \Delta H(t)x(t) + \beta(t)$ and can then be estimated along with the usual objective of estimating $x(t)$. This is done for calibration of the measurements $z(t)$ in the unfailed situation. The calibrated measurements are defined as

$$\begin{aligned} m(t) &= z(t) - \hat{c}(t) \\ &= H(t)x(t) + \epsilon(t) \end{aligned} \tag{2}$$

where

$\hat{c}(t)$ is the estimate of $c(t)$ and
$\epsilon(t) = (c(t) - \hat{c}(t)) + e(t)$ is the additive noise and remaining error associated with the calibrated measurements.

The calibration technique [20] is particularly suitable when scale factor errors evolve slowly in time as compared to the sampling frequency, which may frequently be the case for industrial processes. However, if this situation is not true as it is for inertial navigation systems, the calibration process may require scale factor and bias errors to be separately estimated using nonlinear filtering techniques (for example, see [21]).

If failure decisions are made as a consequence of observing the calibrated measurements, then the occurrence of alarms due to gradual degradation should be significantly reduced and abrupt failures that are large in comparison to the allowable bounds should be easily detected. However, the calibration correction $\hat{c}(t)$ may track the failure in the event of a gradual degradation. Therefore, additional steps must be taken in the failure detection system design to guard against misrepresentation in such an unfavorable situation. This aspect has already been addressed, possible solutions have been experimentally verified in our earlier work [20] and will not be repeated here. In the rest of this section, we present the theoretical development of a novel redundancy management procedure.

For simplicity in notation, we are dropping the indicated time dependence in subsequent mathematical equations by suppressing the underlying t. Thus, equation (2) can be rewritten as

$$m = Hx + \epsilon \tag{3}$$

A measure of relative consistency between redundant measurements is given by the projection of the measurement vector m onto the left null space of the measurement matrix H such that the variations in the underlying component Hx in (3) are eliminated and only the remaining effects of the noise vector ϵ can be observed. An $((l-n) \times l)$ matrix V is chosen such that its $(l-n)$ rows form an orthonormal basis for the left null space of H, i.e.,

$$VH = 0 \quad \text{and} \quad VV^T = I_{l-n} \tag{4}$$

The column space of V is referred to as the "parity space" of H and the projection of m onto the parity space as the "parity vector" [12] which is represented as

$$p = Vm = V\epsilon \tag{5}$$

From (4), it follows that

$$V^T V = I_l - H[H^T H]^{-1} H^T \tag{6}$$

Because of the idempotent property of $V^T V$, the norm of the projection $V^T Vm$ of m onto the left null space of H is identically equal to the norm of p.

The columns, $v_1, v_2, \ldots, v_l$, of V that are projections of the measurement directions (in R^l) onto the parity space are called failure directions since the failure of the ith measurement m_i implies the growth of the parity vector p in (5) in the direction of v_i. For nominally unfailed operations, $\|p\|$ remains small. If a failure occurs, p may (in time) grow in magnitude along the failure subspace, i.e, the subspace spanned by the specific column vectors associated with the failed measurements. If the fault is time-varying, then the failure directions (and hence the failure subspace) may also be time-varying. The increase in the magnitude of the parity vec-

tor signifies abnormality in one or more of the simultaneous redundant measurements and its direction can be used for identification of abnormal measurement(s).

Daly et al. [4] have shown how to make a failure decision using both relative angular orientation and magnitude of projection of the parity vector p with respect to various failure subspaces. In our previous publication [5], computation of angular orientation was specifically avoided by making failure decisions solely dependent on the magnitudes of the projections of p onto distinct subspaces, each orthogonal to one of the failure directions. On this basis, the set of redundant measurements was segregated into "consistent" and "inconsistent" subsets. Although the redundancy management procedure described in [5] has been successfully demonstrated for on-line fault diagnostics in a nuclear reactor, it is only applicable in restrictive situations such as having scalar measurements, using identical error bounds for all redundant measurements, relying on a bilevel fail/no fail characterization, and recursive computation of residuals that require some multiplicative operations. An alternative approach which removes the aforementioned restrictions has been adopted in the current procedure and is explained below.

For $S=\{m_1, m_2, \ldots, m_l\}$, the set of all redundant measurements of an n-dimensional process variable, let S_1 be a proper subset of S consisting of k measurements such that $l<k<n$, and let $S_2 \triangleq (S-S_1)$. Let the projection matrix V in (5) be compatibly partitioned as $V=[V_1 \vdots V_2]$. Let p_2 be the projection of the parity vector $p \epsilon R^{l-n}$ in (5) onto the failure subspace as defined for the measurements in S_2 (i.e., the column space of V_2). The corresponding orthogonal component $p_{2\perp}$ is the projection of p onto the left null space of V_2 and can be represented as

$$p_{2\perp}^T p_{2\perp} = p^T p - p_2^T p_2 \tag{7}$$

In the context of failure detection, $p_{2\perp}$ is more meaningful than p_2 because while p_2 manifests the effects of measurement errors in both S_1 and S_2, it is $p_{2\perp}$ that is influenced solely by the failures in measurements that belong to S_1. This observation follows from Theorem 1 of Appendix A where the norm of the orthogonal component $p_{2\perp}$ is shown to be identical to the norm of the parity vector directly generated from the k measurements in S_1. This implies that the relative proximity (as gauged by an appropriate norm $\|p_{2\perp}\|$) of the parity vector p to the failure subspace of the $(l-k)$ measurements in S_2 can be determined either by computing both $\|p\|$ and $\|p_2\|$ as shown in (7) or by directly computing $\|p_{2\perp}\|$ which is identically equal to the norm of the parity vector generated from the k measurements in $S_1 \triangleq (S-S_2)$. Therefore, if all abnormal measurements are contained in S_2, i.e., S_1 contains only the normal measurements, then $\|p_{2\perp}\|$ should be small implying that the parity vector p is close to the failure subspace of S_2.

In view of the above characterization, the task of fault detection can be recast as determining the largest subset of unfailed measurements or alternatively as determining the failure subspace of smallest dimension such that the projection of the parity vector onto the orthogonal complement of that failure subspace does not indicate the presence of a failure. The uniqueness of a failure subspace of minimum dimension depends upon the number of failed measurements as compared to the total number of redundant measurements. Theorem 2 in Appendix A states that the number of failures occurring at a given sample time that can be uniquely isolated, is less than or equal to $[(l-n)/2]$, i.e., the integral portion of $(l-n)/2$. However, if the number of failures is greater than $[(l-n)/2]$ but less than or equal to $(l-n-1)$, the likely nonuniqueness incurred in this situation needs to be addressed explicitly so that a consistent subset of unfailed measurements may possibly be identified. (The upper bound of $(l-n-1)$ arises because at least $(n+1)$ measurements are required to ascertain consistency between the remaining unfailed measurements at a given sample time.) For example, given seven measurements of a scalar (i.e., $n=1$) variable, three or fewer failures occurring at a sample time can be uniquely isolated; otherwise, for five or fewer nonidentical failures at a sample time the consistent subset of two or more measurements could be identified.

A comprehensive procedure is adopted for identifying an appropriate failure subspace where relative orientation of the parity vector is determined with respect to all possible failure subspaces of dimension $(l-n-1)$ (which is one less than the dimension of the parity space). Equivalently, such information can be generated by checking the internal consistency of individual $(n+1)-$tuplets of measurements. This procedure involves only the computation of magnitudes of associated one-dimensional parity vectors. The basis of this procedure for evaluating internal consistencies of $(n+1)-$tuplets can be explained from the geometry of the bounded region in the $(l-n)-$dimensional parity space, where the parity vector would lie if the set of measurements were in fact consistent. This region in the parity space is the projection of an error cell in R^l where the error vector ϵ should be entirely contained in the absence of any malfunctions, and shall hereinafter be referred to as the consistency region. As illustrated in the example in Appendix B, the consistency region is a polyhedron in the parity space bounded on all sides by hyperplanes comprising the failure subspaces of dimension $(l-n-1)$. Each such hyperplane is the projection of a boundary of the error cell in R^l. The presence of a malfunction can be tested by checking proximity of the parity vector to each of the hyperplanes bounding the polyhedral consistency region. The task of checking proximity involves determining the components of the parity vector orthogonal to the bounding hyperplanes or equivalently testing consistency of each $(n+1)-$tuplet.

We now introduce several definitions to facilitate formal delineation of the proposed concepts of "consistency" and "inconsistency" of any set S of l measurements $(l>n)$ associated with an n-dimensional vector variable relative to all $(n+1)$-tuplets, i.e., distinct subsets of cardinality $(n+1)$ denoted as $s_1, s_2, \ldots, s_v$ where r is given as

$$r = \binom{l}{n+1} \triangleq \frac{l!}{(n+1)!(l-n-1)!} \tag{8}$$

The magnitude of the parity vector p_i of dimension one, generated from $(n+1)$ measurements in the $(n+1)$-tuplet s_i, $i=1, 2, \ldots r$, is a measure of inconsistency of the $(n+1)$ measurements that belong to s_i.

Definition 1: The inconsistency index $\xi(t)[s_i]$ of the $(n+1)$-tuplet s_i at sample time t is a real number directly related to the magnitude of its parity vector $p_i(t)$. Thus, after dropping the time dependence notation for brevity, the inconsistency index can now be expressed as

$$\xi : s_i \rightarrow [0, \infty), \; i=1,2, \ldots \ldots, r \tag{9}$$

The exact structure of ξ is dependent on the specific noise statisics as well as on the detection algorithm which may be recursively implemented. Furthermore, ξ is appropriately scaled such that under nominal conditions $\xi[s_i] \leqq 1$ for every i. For example, ξ could be the (scaled) generalized log-likelihood ratio in sequential probability ratio test [18]. Another example is the single sample test of amplitude-limited noise where

$$\xi[s_i] = |p_i| / \theta_i \tag{10}$$

and

$$\theta_i \triangleq \sum_{j=1}^{n+1} |v_i^j| \, b_i^j$$

and v_i^j is the jth element of the $1 \times (n+1)$ projection matrix V_i associated with s_i, and b_i^j is the specified error bound of the jth measurement in s_i.

Definition 2: An $(n+1)$-tuplet s_i, $i=1,2 \ldots . r$ is defined to be internally consistent if its inconsistency index is less than or equal to unity, i.e., $\xi[s_i] \leqq 1$.

Definition 3: A set of measurements is defined to be consistent if each of its $(n+1)$-tuplets is internally consistent.

Definition 4: Two disjoint subsets S_1 and S_2 of a measurement set S are defined to be relatively inconsistent if there exists no internally consistent $(n+1)$-tuplet having at least one element from each of S_1 and S_2.

Remark: The concept of relative inconsistency of the disjoint subsets S_1 and S_2, where further $(S_1 \cup S_2) = S$, is exemplified as follows in terms of the internal consistencies of its $(n+1)$-tuplets, $s_1, s_2, \ldots, s_r$, where r is as in equation (8).

Let C be the $r \times l$ consistency matrix defined as

$$C_{ij} = \begin{cases} 1 & \text{if } m_j \epsilon s_i \text{ and } \xi[s_i] \leqq 1 \\ 0 & \text{otherwise} \end{cases} \tag{12}$$

Then, $s_1, s_2, \ldots, s_r$ can be reordered in a manner that allows the partitioning of C as

$$C = \left[\begin{array}{c|c} C_1 & 0 \\ \hline 0 & C_2 \\ \hline 0 & 0 \end{array}\right] \tag{13}$$

where the first and second sets of columns correspond to S_1 and S_2 respectively, and C_1 and C_2 are the only nonzero submatrices.

Definition 5: A set of measurements that is not consistent is defined to be inconsistent [moderately consistent] if the set can [cannot] be split into two or more relatively inconsistent subsets.

Remark: The concept of moderate consistency is germane to the situation when errors in some of the measurements are in the vicinity of their respective error bounds such that the measurements are contiguously dispersed and no measurement appears to be clearly malfunctioning (i.e., in the words of classical statistics their are no obvious outliers). The notion of moderate consistency can also be explained with the aid of the consistency matrix C if it is impossible to partition C into submatrices in the manner illustrated in (13) to demonstrate relative inconsistency.

The above definitions and the associated separation schemes for decomposing all measurements obtained according to these rules serve primarily in the isolation of inconsistent measurements. From the subset of any remaining measurements which are either consistent or moderately consistent, it is possible to extract a consistent subset. Identification of such a consistent subset is achieved by determining the direction of the parity vector and not by its magnitude. To this end, we introduce three additional definitions.

Definition 6: Degree of inconsistency $D(S)$ of a measurement set S is the largest of the inconsistency indices associated with each of its $(n+1)$-tuplets, i.e., $D(S) = \text{Max}\xi[s_i]$.

Remark: S is consistent iff $D(S) \leqq 1$.

Remark: The degree of inconsistency is a single scalar measure of the consistency of the entire measurement set and can be geometrically interpreted as the inverse of the amount by which the parity vector should be multiplied so that it lies on the surface of the polyhedral consistency region.

Definition 7: Given a nonempty subset T of S, the relative degree of inconsistency, $D(T;S)$, of T with respect to S is defined to be the largest inconsistency index of all $(n+1)$-tuplets of S, that contains at least q elements of T where $q = \text{Min}\ (\#T, n)$ and $\#T$ denotes the cardinality of T.

Remark: $D(T;S)$ is a measure of relative consistency between the subsets T and $S-T$; and $D(T;S) > 1$ if T and $S-T$ are relatively inconsistent. The inconsistency indices of the $(n+1)$-tuplets, if any, of T are taken into account in determining $D(T;S)$ whereas the inconsistency indices of the $(n+1)$-tuplets of $S-T$ have no direct bearing on the evaluation of $D(T;S)$.

Definition 8: A nonempty subset T of S is defined to be a most relatively consistent subset of S if T has the least relative degree of inconsistency amongst all subsets of S.

Remark: Theorem 3 in Appendix A states that there exists an n-tuplet which is a most relatively consistent subset of S. Determination of a most relatively consistent n-tuplet is equivalent to the midvalue selection process in the thresholdless redundancy management procedure proposed by Potter and Suman [12, 13].

3 On-Line Application to Nuclear Reactors

The redundancy management procedure was experimentally verified by demonstration of on-line failure detection and isolation in the 5 MWt nuclear reactor MITR-II [22] operated by Massachusetts Institute of Technology as well as in the 62.5 MWt liquid metal fast breeder reactor EBR-II [23] operated by Argonne National Laboratory. Since scalar process variables are routinely encountered in nuclear reactors, the real-time failure detection computer program used in our experimentation was limited to scalar variables only to match the application. In line with the rationale and definitions presented in the previous section, a real-time computer code has been developed for concurrent checking of consistencies between all redundant measurements of a given variable at each sample time; the algorithm of the implementation is outlined in Appendix C. Two alternative sequential test procedure implementations, each of which utilizes the algorithm of Appendix C, were devised for failure detection under both steady-state and transient operations. Built-in tests such as limit checks and rate checks for each redundant measurement were routinely incorporated within these test procedures. The first alternative implementation used a fixed sample approach but no assumptions were invoked regarding the measurement noise statistics except that the noise being amplitude-limited with known error bounds. In the second alternative implementation we used Chien's sequential test algorithm [17] where the number of test samples were not fixed a priori. However, the measurement noise distribution was assumed to be Gaussian. We adopted the first alternative for actual use because, although not optimal, it is computationally more efficient than the second and is expected to be more robust since the actual noise distribution is anticipated to be non-Gaussian. The a priori fixed number of samples and the error bounds needed for the first alternative should be selected to limit the probability of false alarms to a low value (typically 1.0E-06). The consequent delay in detecting a gradually degrading measurement was still tolerable because the fault detection procedure was carried out in conjunction with the calibration filter [20] (its possible use being mentioned in Section 2 following equation (2)). The filter adaptively reduces the weight ascribed to the degraded measurement for estimation of the measured variable until a fault is detected. This issue is discussed in detail in [20].

For MITR-II, the fault detection procedure was similar to that reported in our earlier paper [5] except that the algorithm for checking consistency of redundant measurements was replaced by that described in Appendix C. The experimentally deduced results were similar to those reported earlier [5] and are not repeated here. The experimentation of EBR-II was conducted for validating the sensor signals and for detecting malfunctions of plant components in the primary coolant (sodium) loop. The experimentation was conducted over a

wide range of steady-state operations as well as for transient conditions related to reactor shutdown. A detailed description of the experiments and further discussion of significant results are presented in [24].

The failure detection procedure proposed in this paper has also been applied to the simulation of boiling water reactor (BWR) suppression pool temperature monitoring [25] and is currently being implemented for real-time signal validation of a commercial pressurized water reactor (PWR) plant. Further applications of this failure detection technique have occurred outside the United States [26].

Summary and Conclusions

The paper presents the theory from a geometric and an algebraic view-point and application of a redundancy management procedure for fault detection and isolation in time-dependent processes, where the measured variables may be vector or scalar quantities. In order to apply this procedure there should be redundant measurements of the process variable under consideration, which could be direct sensor outputs and/or indirect analytically derived measurements. The resulting redundancy management procedure reported in this paper is essentially independent of the fault detection strategy and measurement noise statistics, and builds upon the concept of partitioning the measurement set into so-designated "consistent" and "inconsistent" subsets for estimation and fault isolation, respectively. This operation is performed in a systematic way by checking for consistency within all subsets of $(n+1)$ measurements where n is the dimension of the underlying measured variable.

The procedure has been verified by both simulation and prototype implementation in nuclear reactors and has been found to be acceptable for real-time detection and isolation of faulty sensors and plant equipment using commercially available microcomputers. Since the procedure does not require any arithmetic multiplications (at least for scalar variables) for fault detection and isolation, it is computationally fast and appears to be suitable for on-line applications in other industrial processes.

Acknowledgment

The authors acknowledge benefits of discussions with Dr. J. J. Deyst of the C.S. Draper Laboratory, and the assistance of Professor D. D. Lanning, Dr. J. A. Bernard, and the staff of the MIT Research Reactor in the experimental phase of this work. The authors are especially grateful to one of the anonymous reviewers for his/her excellent comments.

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 Kerr, T. H., "The Controversy over the Use of SPRT and GLR Techniques and Other Loose-Ends in Failure Detection," *Proceedings of American Control Conference*, June 1983, pp. 966–977.

3 Chow, E. C., and Willsky, A. S., "Analytical Redundancy and the Design of Robust Failure Detection Systems," *IEEE Trans. Aut. Contr.*, Vol. AC-29, July 1984, pp. 603–614.

4 Daly, K. C., Gai, E., and Harrison, J. V., "Generalized Likelihood Test for FDI in Redundant Sensor Configurations," *Journal of Guidance and Control*, Vol. 2, No. 1, Jan.-Feb. 1979, pp. 9–17.

5 Ray, A., Desai, M., and Deyst, J., "Fault Detection and Isolation in a Nuclear Reactor," *Journal of Energy*, Vol. 7, No. 1, Jan.-Feb. 1983, pp. 79–85.

6 Desai, M., and Ray, A., "A Fault Detection and Isolation Methodology – Theory and Application," *Proceedings of American Control Conference*, June 1984, pp. 262–270.

7 Tylee, J. L., "A Generalized Likelihood Ratio Approach to Detecting and Identifying Failures in Pressurizer Instrumentation," *Nuclear Technology*, Vol. 56, Mar. 1982, pp. 482–492.

8 Clark, R. N., and Campbell, B., "Instrument Fault Detection in a Pressurized Water Reactor Pressurizer," Nuclear Technology, Vol. 56, Jan. 1982, pp. 23–32.

9 Kitamura, M., "Detection of Sensor Failures in Nuclear Plants Using Analytic Redundancy," *Trans. Am. Nuc. Soc.*, Vol. 34, 1980, pp. 581–584.

10 Ray, A., Geiger, R., Desai, M., and Deyst, J., "Analytic Redundancy for On-Line Fault Diagnosis in a Nuclear Reactor," *Journal of Energy*, July/Aug. 1983, pp. 367–373.

11 Deckert, J. C., Fisher, J. L., Laning, D. B., and Ray, A., "Signal Validation for Nuclear Power Plants," ASME JOURNAL OF DYNAMIC SYSTEMS, MEASUREMENT, AND CONTROL, Mar. 1983, pp. 24–29.

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

13 Potter, J. E., and Suman, M. C., "Extension of the Midvalue Selection Technique for Redundancy Management of Inertial Sensors," *Journal of Guidance, Control, and Dynamics*, Vol. 9, No. 1, Jan./Feb. 1986, pp. 37–44.

14 Schweppe, F. C., *Uncertain Dynamic Systems*, Prentice-Hall, Englewood Cliffs, NJ 1973.

15 Wald, A., *Sequential Analysis*, John Wiley, New York, 1947.

16 Shiryaeyev, A. N., *Optimal Stopping Rules*, Springer-Verlag, New York, 1978.

17 Chien, T. T., and Adams, M. B., "A Sequential Failure Detection Technique and Its Application," *IEEE Trans. Aut. Contr.*, Vol. AC-21, No. 5, Oct. 1976, pp. 750–757.

18 Ray, A., Desai, M., and Deyst, J., "On-Line Fault Diagnosis in a Nuclear Reactor by Sequential Testing," *IEEE Trans. Nuc. Sci.*, Vol. NS-30, June 1983, pp. 1850–1855.

19 Spayer, J. L., and White, J. E., "The Shiryaev Sequential Probability Ratio Test for Redundancy Management," *Journal of Guidance, Control, and Dynamics*, Vol. 7, No. 5, Sept./Oct. 1984, pp. 588–595.

20 Ray, A., and Desai, M., "A Calibration and Estimation Filter for Multiply Redundant Measurement Systems," ASME JOURNAL OF DYNAMIC SYSTEMS, MEASUREMENT, AND CONTROL, June 1984, pp. 149–156.

21 Hall, S. R., et al., "Inflight Parity Vector Compensation for FDI," *Proceedings of National Aerospace and Electronics Conference* (NAECON) May 1982, pp. 380–387.

22 Reactor Systems Manual, Report No. MITNRL-004, MIT Nuclear Reactor Laboratory, Massachusetts Institute of Technology, 1980.

23 Metcalf, E. E., et al., EBR-II System Design Description, Volume II, Primary System, Chapter 3, Primary Cooling System, Argonne National Laboratory, June 1971.

24 Deutsch, O. L., Ornedo, R. S., and Lindsay, R. W., "Implementation of Real-Time Signal Validation at EBR-II," *Trans. Am. Nuc. Soc.*, Vol. 45, Oct./Nov. 1983, pp. 660–661.

25 Fisher, J. L., et al., "Signal Validation for a BWR Suppression Pool," *Trans. Am. Nuc. Soc.*, Vol. 44, Suppl. 1, Aug. 1983, pp. 50–51.

26 Swingelstein, G., Bath, L., and Adam, T., "Application of the Parity Space Technique to the Validation of the Water Level Measurement of Pressurizer for Steady State and Transients," *Proceedings of the Fifth Power Plant Dynamics, Control, and Testing Symposium*, Knoxville, TN, Paper No. 28, Mar. 1983.

27 Bryson, A. E., and Ho, Y. C., *Applied Optimal Control*, Blaisdell, Waltham, MA, 1969.

APPENDIX A

Theorem 1: Let $v_1, v_2, \ldots, v_l$ represent the failure directions in the parity space corresponding to the set of redundant measurements $\{m_1, m_2, \ldots, m_l\}$ of an n-dimensional variable. The norm of the projection of the $(l-n)$-dimensional parity vector (generated by all l measurements) onto the $(k\text{-}n)$-dimensional subspace that is orthogonal to the subspace spanned by $v_{k+1}, v_{k+2}, \ldots, v_l$, is identically equal to the norm of the $(k-n)$-dimensional parity vector that is generated by the set of k measurements $\{m_1, m_2, \ldots, m_k\}$ where $n<k<l$.

Proof: The measurement vector m, measurement matrix H, and projection matrix V in (3) and (4) are compatibly partitioned as follows:

$$m^T = [\mu_1^T | \mu_2^T],\ H^T = [H_1^T | H_2^T],\ \text{and}\ V = [V_1 | V_2] \qquad \text{(A.1-1)}$$

where μ_1 is the $(k \times 1)$ vector comprising k measurements and μ_2 is the $((l-k) \times 1)$ vector comprising the remaining measurements. From (3) it follows that

$$\mu_1 = H_1 x + \epsilon_1 \qquad \text{(A.1-2)}$$

where the $(k \times n)$ matrix H_1 is of rank n. The $(k-n)$-dimensional parity vector $\tilde{p}$ for the set of k measurements is given by (5) as

$$\tilde{p} = \tilde{V}\mu_1 \qquad \text{(A.1-3)}$$

where $\tilde{V}$ has the properties given by (4) and (6) that:

$$\tilde{V}H_1 = 0, \quad \tilde{V}\tilde{V}^T = I_{k-n}, \quad \text{and} \quad \tilde{V}^T\tilde{V} = I_k - H_1(H_1{}^TH_1)^{-1}H_1^T \tag{A.1-4}$$

Since $(H_1^TH_1)^{-1} = (H^TH - H_2^TH_2)^{-1}$, application of the matrix inversion lemma [27] yields

$$(H_1^TH_1)^{-1} = B + BH_2^T(I_{l-k} - H_2BH_2^T)^{-1}H_2B \tag{A.1-5}$$

where $B \triangleq (H^TH)^{-1}$. Substituting (A.1-5) in (A.1-4) results

$$\tilde{V}^T\tilde{V} = (I_k - HBH_1^T) - H_1BH_2^T(I_{l-k} - H_2BH_2^T)^{-1}H_2BH_1^T \tag{A.1-6}$$

Using the relationship $V^TV = I_l - HBH^T$ expressed in partitioned form, (A.1-6) can be further simplified as

$$\tilde{V}^T\tilde{V} = V_1^T(I_{l-n} - V_2(V_2^TV_2)^{-1}V_2^T)V_1 \tag{A.1-7}$$

Let G be a $(k-n) \times (l-n)$ matrix such that the rows of G form an orthonormal basis for the left null space of V_2, i.e., the subspace orthogonal to the failure directions v_{k+1}, v_{k+2}, . . . , v_l. Therefore, G has the properties given by (4) and (6):

$$GV_2 = 0, \; GG^T = I_{k-n}, \quad \text{and } G^TG = I_{l-n} - V_2(V_2^TV_2)^{-1}V_2^T \tag{A.1-8}$$

The projection matrix $\tilde{V}$ in (A.1-3) can be chosen to be identical to GV_1 because GV_1 satisfies the properties in (A.1-4). Then, the projection of the parity vector p onto the column space of G is

$$Gp = GVm = G[V_1 \vdots V_2]\begin{bmatrix}\mu_1 \\ -- \\ \mu_2\end{bmatrix} = GV_1\mu_1 = \tilde{V}\mu_1 = \tilde{p} \tag{A.1-9}$$

The proof is completed by arguing that the norm of the projection of p onto the left null space of V_2 is identically equal to $\|Gp\|$. ■

Corollary to Theorem 1: The residual vector $\tilde{\eta} \triangleq \tilde{V}^T\tilde{p}$ for the measurement set $\{m_1, m_2, \ldots, m_l\}$ is related to the residual vector $\eta \triangleq V^Tp$ for all measurements as $\tilde{\eta} = \eta_1 - V_1^TV_2(V_2^TV_2)^{-1}\eta_2$, where $\eta^T = [\eta_1^T \vdots \eta_2^T]$ is an appropriate partitioning.

Proof:

$$\begin{aligned}\tilde{\eta} &= \tilde{V}^T\tilde{p} = \tilde{V}^TGp = V_1^TG^TGp \\ &= V_1^Tp - V_1^TV_2(V_2^TV_2)^{-1}V_2^Tp\end{aligned} \tag{A.1-10}$$

The proof follows by substituting $\eta_1 = V_1^Tp$, and $\eta_2 = V_2^Tp$ in (A.1-10). ■

Theorem 2: Given l redundant measurements of an n-dimensional variable at a sample time, the number q of failed measurements that can be uniquely isolated is given as $2q \leqq (l-n)$, i.e., $q \leqq [(l-n)/2]$ where [*] indicates the integral part of *.

Proof: For unique isolation of q failures in a set of l redundant measurements, one and only one subset of cardinality $(l-q)$ that contains the unfailed measurements must exhibit consistency. However, only $(l-q-n)$ failure directions are needed to span the $(l-q-n)$-dimensional parity space that is generated from a subset of $(l-q)$ measurements. Therefore, situations may arise where a subset of cardinality $(l-q)$ containing more than $(l-q-n)$ failed measurements may exhibit consistency, i.e., if $q > (l-q-n)$. This implies that $q \leqq (l-q-n)$ or $2q \leqq (l-n)$ for unique isolation. ■

Theorem 3: Given a set S of l measurements of an n-dimensional variable such that $l > n$, there exists an n-tuplet which is a most relatively consistent subset of S. (See Definition 8.)

Proof: Let a j-tuplet $(1 \leqq j \leqq l)$ be denoted as $S^j \subset S$. With respect to a given S^j, let an i-tuplet be denoted as S_j^i if $S_j^i \subset S$ or as $\tilde{S}_j^i$ if $\tilde{S}_j^i \subset (S - S^j)$. From Definitions 1, 6, and 7, it follows that

$$D(S^j;S) = \operatorname{Max}_{S_j^k} \operatorname{Max}_{\tilde{S}_k^{n+1-k} \subset (S - S_j^k)} \xi[s_j^k \cup \tilde{S}_k^{n+1-k}] \tag{A.3-1}$$

where $k = \operatorname{Min}(j,n)$.

By Definition 8, a most relatively consistent subset Θ satisfies the following condition

$$D(\Theta) = \operatorname*{Min}_{1 \leqq j \leqq l} \operatorname*{Min}_{S^j} D(S^j;S) \tag{A.3-2}$$

To show that there exists an n-tuplet which satisfies (A.3-2), we consider two cases.

Case 1: For $1 \leqq j \leqq n$, i.e., $k = \min(j,n) = j$ in Definition 8.

Let $X(S^j)$ be the collection of all $(n+1)$-tuplets $S^j \cup \tilde{S}^{n+1-j}$ generated from a given j-tuplet S^j. Substituting j for k in (A.3-1), it follows that

$$D(S^j;S) = \operatorname*{Max}_{\varphi \epsilon X(S^j)} \xi[\varphi] \tag{A.3-3}$$

By use of Lemma 1 in (A.3-3), it follows that

$$D(S^{j+1};S) \geqq D(S^j;S) \text{ if } S^j \subset S^{j+1} \text{ and } 1 \leqq j < n \tag{A.3-4}$$

From (A.3-4), it suffices to observe that

$$\operatorname*{Min}_{S^n} D(S^n;S) \geqq \operatorname*{Min}_{S^j} D(S^j;S) \text{ for } 1 \leqq j < n \tag{A.3-5}$$

Case 2: $n \leqq j \leqq l$, i.e., $k = \min(j,n) = n$ in Definition 8.

Let $Y(S^j)$ be the collection of all $(n+1)$-tuplets $S_j^n \cup \tilde{S}_n^1$. (Note that $\tilde{S}_n^1$ is a set of cardinality 1 and is given as $\tilde{S}_n^1 \subset (S - S_j^n)$.) Substituting n for k in (A.3-1), it follows that

$$D(S^j;S) = \operatorname*{Max}_{\varphi \epsilon Y(S^j)} \xi[\varphi] \tag{A.3-6}$$

By use of Lemma 2 in (A.3-6), it follows that

$$D(S^j;S) \geqq D(S^{j+1};S) \text{ if } S^j \subset S^{j+1} \text{ and } n \leqq j < l. \tag{A.3-7}$$

From (A.3-7), it suffices to observe that

$$\operatorname*{Min}_{S^n} D(S^n;S) \geqq \operatorname*{Min}_{S^j} D(S^j;S) \text{ for } n \leqq j \leqq l. \tag{A.3-8}$$

Combining (A.3-5) and (A.3-8), it follows that

$$\operatorname*{Min}_{S^n} D(S^n;S) \geqq \operatorname*{Min}_{S^j} D(S^j;S) \text{ for } 1 \leqq j \leqq l. \tag{A.3-9}$$

Thus, there exists an n-tuplet which satisfies (A.3-2). ■

Lemma 1 [of Theorem 3]: If $S^j \subset S^{j+1}$ and $1 \leqq j < n$, then $X(S^{j+1}) \subset X(S^j)$.

Proof: Let $q \notin S^j$ and $S^{j+1} = S^j \cup \{q\}$. This implies that $q \notin (S - S^{j+1})$ and $(S - S^j) = (S - S^{j+1}) \cup \{q\}$. For every $\tilde{S}_{j+1} \subset (S - S^{j+1})$, there exists an $\tilde{S}_j^{n+1-j} \subset (S - S^j)$ such that $\tilde{S}^{n+1-j} = \tilde{S}_{j+1}^{n-j} \cup \{q\}$. Thus, every $(n+1)$-tuplet $(S^{j+1} \cup \tilde{S}_{j+1}^{n-j}) \epsilon X(S^{j+1})$ is contained in $X(S^j)$. ■

Lemma 2 [of Theorem 3]: If $S^j \subset S^{j+1}$ and $n < j < l$, then $Y(S^j) \subset Y(S^{j+1})$.

Proof: Since $S^j \subset S^{j+1}$, for every S_j^n there exists an S_{j+1}^n such that $S_{j+1}^n = S_j^n$. Thus, every $(n+1)$-tuplet $(S_j^n \cup \tilde{S}_n^1) \epsilon Y(S^j)$ is contained in $Y(S^{j+1})$. ■

APPENDIX B

Geometric Interpretation of the Redundancy Concept

A geometric representation of the redundancy management concept that is the cornerstone in this paper is illustrated in Figs. B-1 and B-2 for a set of three redundant measurements of a scalar variable (e.g., $n = 1$ and $H = [1\ 1\ 1]^T$) with the noise amplitudes in the measurements m_1, m_2, and m_3 being assumed to be limited by error bounds, b_1, b_2, and b_3, respectively. However, the concept is not restricted to the assumption of amplitude-limited noise. For example, in more flexible situations as discussed in [18], the error bounds should be replaced by appropriate thresholds if a sequential fault detection strategy is used along with this redundancy management procedure.

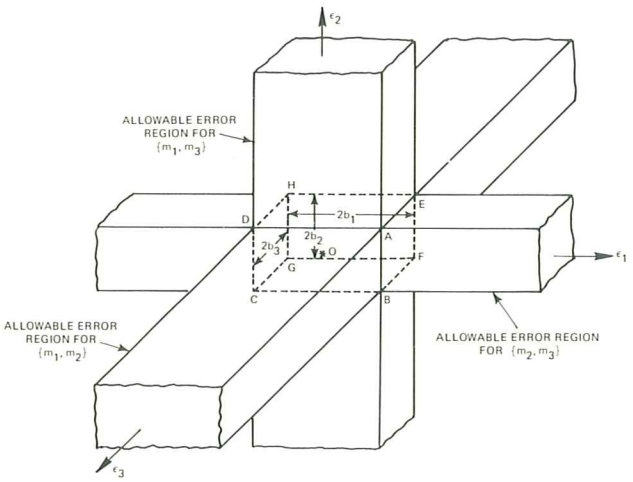

Fig. B1 Allowable error region in the measurement space

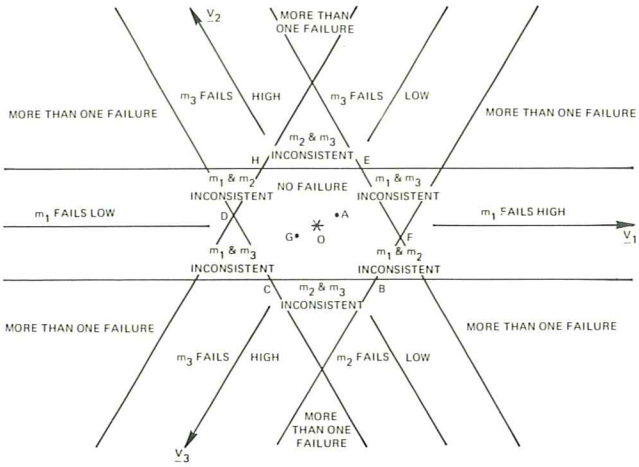

Fig. B2 Division regions in the parity space

Figures B-1 and B-2 show the parity space projections of the consistency regions for the distinct pairs of measurements within which measurement errors are assumed to be contained for normally functioning measurements. Each consistency region is an infinite prism of rectangular cross section with the axis along the direction of measurement not included in the respective pair, and is seen to be divided into three regions of interest. The region centered around the origin in Fig. B-1 is a 3-cell of sides $2b_1$, $2b_2$, and $2b_3$ representing consistency region for the measurements m_1, m_2, and m_3 and is shared by all three prisms. The other two semi-infinite regions within a prism on either side of the 3-cell represent the inconsistency region for the measurement that is not included in the pair associated with the prism.

Figure B-2 shows the projections of the consistency regions of different sets of measurements on the parity space which, in this particular case, is the plane orthogonal to the direction $[1\ 1\ 1]^T$ in the 3-dimensional measurement space. In this plane, the projection is unaffected by changes in the measured variable x. Three infinite strips centered along the three failure directions are the projections of the three infinite prisms and are seen to divide the parity space into several regions. The hexagonal region, surrounding the origin, is formed by the intersection of the three infinite strips. This hexagon is also the projection of the error 3-cell and is the region of validity for all three measurements. The six triangular regions on the six sides of the hexagon, that are formed by the intersection of only two of the three strips, represent the regions of moderate consistency where a measurement, say m_1, exhibits consistency with respect to the remaining two measurements, m_2 and m_3, which themselves are relatively inconsistent. Each of the remaining semi-infinite regions of the strips corresponds to the failure of a specific measurement. The remaining part of the parity space, not covered by the three infinite strips, that consists of six semi-infinite forks implies failure of more than one measurement with no possibility of unique failure isolation.

APPENDIX C

Redundancy Management Algorithm for Scalar Measurements

In many industrial applications such as aircraft turboengines, power plants, and chemical processes, the measured variables are scalar quantities such as pressure, temperature, and power, i.e., $n=1$ and x is scalar in (1). The measurement matrix in (3) can be expressed, without loss of generality, as $H=[1\ 1\ 1\ \ldots\ 1]^T$. In the context of the definitions introduced in the Section 2 of the main text, a set of k redundant measurements is consistent if all $k(k-1)/2$ pairs are consistent. It is important to note that the redundancy management procedure is independent of the criterion for determination of consistency of a measurement pair. For example, the afore-said criterion could be a simple single-sample test based on allowable error bounds or a sequential test using recursive relations based on the generalized likelihood ratio test.

A real-time algorithm for the redundancy management procedure has been developed and verified by experimentation at operating nuclear reactors [22, 23]. It does not need any multiplicative arithmetic operations. The set of redundant measurements is partitioned into appropriate subsets on the basis of two consistency numbers for each measurement. The algorithm is briefly outlined below.

1. Order the redundant measurements of the scalar variable such that $m_1 <= m_2 <= \ldots\ldots <= m_l$.
2. Determine consistency numbers

$$N_i^+ = \sum_{j=i+1}^{l} \chi[\text{pair } m_i \text{ and } m_j \text{ consistent}],\ i=1,2,\ldots,(l-1)$$

$$N_i^- = \sum_{j=1}^{i-1} \chi[\text{pair } m_i \text{ and } m_j \text{ consistent}],\ i=2,3,\ldots\ldots,l.$$

where, in the above, the indicator function χ is defined as

$$\chi[*] = \begin{cases} 1 \text{ if } * \text{ is true} \\ 0 \text{ if } * \text{ is false.} \end{cases}$$

and $N_l^+ = N_1^- = 0$.

3. (i) The set is consistent if $N_i^+ + N_i^- = l-1$ for every i.
   (ii) m_i is inconsistent with respect to each of the remaining $(l-1)$ measurements if $N_i^+ + N_i^- = 0$.
   (iii) The set consists of relatively inconsistent subsets if there exists a measurement m_j such that $N_j^+ = N_j^- = 0$. Specifically, the subsets $\{m_1, \ldots, m_{j(1)}\}$, $\{m_{j(1)+1}, \ldots, m_{j(2)}\}$, $\ldots$, $\{m_{j(q)+1}, \ldots, m_l\}$ are mutally incosnsitent and each of the above subsets is either "consistent" or "moderately consistent" (see Definition 5) only if there exists $j(1)<j(2)<\ldots\ldots<j(q)$ such that $N_{j(k)}^+ = N_{j(k)+1}^- = 0$ for $k=1,2,\ldots,q$.