Fault Detection and Isolation in a Nuclear Reactor

Asok Ray,* Mukund Desai,† and John Deyst‡
The Charles Stark Draper Laboratory, Inc., Cambridge, Massachusetts

A fault detection and identification methodology has been developed for sensor and plant component validation, with special emphasis on applications to nuclear powerplants. The methodology is particularly suitable for on-line fault diagnostics and does not rely on detailed knowledge of sensor and plant noise statistics. The algorithm has been computer coded for real-time applications and validated by on-line demonstration in an operating nuclear reactor.

Introduction

VARIOUS methods for fault detection and identification (FDI) of sensors have been reported in the literature.[1-4] However, current practice in the nuclear industry is restricted to a few rather rudimentary techniques such as like-sensor comparisons, limit checking, auctioneering, etc. Although these techniques generally serve to improve system safety, availability, and operability, some limitations, such as the inability to identify gradual drifts and to detect common mode failures, significantly curtail their effectiveness. (If two or more elements fail identically, due to a common cause, the failure is called common mode.)

The above limitations can often be circumvented with the aid of advanced computer-aided diagnostic techniques that have been developed for aerospace systems. In addition to improvement of plant availability and operability, these techniques promise to aid plant operators in making valid and timely decisions, thereby enhancing plant safety.

The FDI methodology reported in this paper is developed on the basis of the "parity space" concept,[3] which takes into account inconsistencies among all data sources. Any malfunctioning sensors are isolated by sequential checking until a relative consistency among the remaining (normal) sensors is achieved. This methodology does not require a detailed knowledge of sensor and plant noise statistics. Error bounds that are allowed for normal operation of the sensors are sufficient for making decisions.

Real-time computer codes have been developed for detection and identification of failed sensors and plant components. As a proof of concept, these codes were verified by demonstration of on-line detection and identification of sensor failures in the 5 MW(t) nuclear reactor presently in operation at MIT, Cambridge, Mass.

Background of the Fault Detection and Isolation Methodology

Various FDI methods in dynamical systems[1-4] exploit several forms of available redundant data. Redundancy can be broadly classified into two groups:

1) Directly redundant data when two or more sensors measure the same variable.

2) Analytically redundant data when additional evaluation of the variable is indirectly available from the physical relationships among other directly or indirectly measured variables.

For example, two sensors may be available for measurement of coolant temperature in a nuclear reactor, and a mathematical model of the thermal-hydraulic process in the reactor may be formulated to obtain analytically redundant data. Thus installation of an additional temperature sensor solely for the purpose of fault isolation may be avoided.

Most of the reported FDI methods[2,4] are formulated on the basis of certain statistical assumptions, such as Gaussian distribution of noise, and may not be suitable for many industrial applications where the statistical characteristics of sensor and plant component noise may not follow any specific pattern and are known only to the extent of the manufacturer's specifications. Usually the available information on tolerances due to calibration, nonlinearity, scale factors, etc., is sufficient to quantify a symmetric error bound; i.e., if the sensor output error does not exceed the bound, the device is assumed to be functioning normally.

The FDI methodology reported in this paper systematically seeks the largest consistent subset from a set of measurements. The estimate of the measured variable is obtained from the consistent subset and the inconsistent measurements, if any, are isolated. For example, consistency between the outputs of two sensors measuring the same variable implies that the outputs differ by less than the sum of their error bounds and conversely. However, as the number of measurements increases, the checking of consistency in all possible combinations [equal to $\ell(\ell-1)/2$ for all ℓ measurements] and the attendant task of bookkeeping for the consistent and inconsistent measurements for the purpose of fault isolation becomes cumbersome. An alternative method, which is systematic and computationally more efficient for the great majority of situations, has been developed on the basis of the "parity-space" concept.[3] A preliminary version of this methodology was also applied to the simulation of signal validation in powerplants.[5]

The development of the FDI methodology, formulation of a real-time algorithm, and its limitations are described in Appendix A, along with a simple geometric representation.

Application of the FDI Methodology to a Nuclear Reactor

On-line verification of the FDI methodology was demonstrated in the 5 MW(t) nuclear reactor, MITR-II, presently in operation at MIT. A detailed description of the reactor configuration and instrumentation is given in the MITR-II manual.[6] For illustration of the FDI methodology as limited to the primary coolant system, a simplified diagram of the process and instrumentation is given in Fig. 1.

The MITR-II[6] is heavy-water reflected and light-water cooled and moderated and functions as a research and educational facility at MIT. The reactor power level is controlled by one regulating rod and a shim blade assembly that

Received Aug. 20, 1981; revision received Dec. 22, 1981.

*Staff Member.
†Staff Member. Member AIAA.
‡Division Leader. Member AIAA.

can be moved up and down separately by electrical motors. The shim blade assembly consists of six boron-impregnated stainless steel plates. Under scram conditions, both the rod and shim blade assembly can be dropped within a fraction of a second.

Heat generated by the fission of U^{235} is removed from the core by the primary light-water cooling system. The heated water leaving the reactor core is force-circulated by electrically driven pumps through a bank of heat exchangers and back to the reactor inlet plenum. The heat exchangers transfer heat from the primary coolant to the secondary light-water coolant which, in turn, dissipates heat to the atmosphere by means of two forced-air-circulated cooling towers that operate in parallel.

The nuclear instrumentation under consideration consists of three neutron flux sensors and a gamma-ray sensor that measures neutron power from radioactivity of the primary coolant water. All four sensors are linear over the power range. Four measurements of primary coolant flow are obtained from the pressure differences across orifices and restrictions. The primary coolant flow in this reactor is practically constant under all operating conditions. Primary coolant temperatures are measured as follows: one sensor for hot-leg temperature, one sensor for cold-leg temperature, and one sensor for temperature difference between the legs. In effect, two sources of information for temperature difference are available from direct measurements. These 11 sensors are hard-wired to a MINC-11 minicomputer through analog-digital (A/D) converters and appropriate signal conditioners. To eliminate the effects of any malfunctioning in the fault diagnostic equipment on the reactor operation, the crucial sensors are buffered by signal isolators.

Figure 1 shows that sufficient direct redundancies exist for fault isolation and measurement validation for neutron power and primary coolant flow, but there is dual redundancy only for the hot-leg to cold-leg temperature difference, which is inadequate for isolation of a fault. Therefore, a third measurement for temperature difference was analytically obtained from a thermal-hydraulic model of the primary coolant system. Failure of one of the two temperature difference sensors can thus be isolated from the consistency between the good sensor and the analytic measurement. On the other hand, an inconsistency of the analytic measurement with two mutually consistent sensors implies possible malfunctioning of some plant components. The actual cause of inconsistency can usually be resolved with the aid of other additional information.

The thermal-hydraulic model of the primary coolant system is formulated from the analytic relationship among different process variables that include validated measurements of neutron power and primary coolant flow obtained from the direct measurements. Other variables used in the model are secondary coolant and ambient temperatures which are presently not hard-wired to the computer but entered as input data. The analytic measurement for temperature difference was validated with appropriate sensor outputs for transient conditions following movements of the shim blade assembly, as well as for various steady-state levels within the normal operating range. The accuracy of the analytical measurement was found to be comparable to that of the sensors, thus justifying its use together with two direct measurements for the purpose of fault isolation and measurement validation.

Tests for verifying the FDI methodology were conducted for both steady-state and transient conditions. Symmetric error bounds for the measurements where chosen on the basis of process noise, spatial location of sensors, and tolerances due to scale factor, nonlinearities, calibration, etc. These error bounds were relaxed to some extent under transient operations to account for possible dynamic errors in the measurements. Nominal values and error bounds for neutron power, primary coolant flow, and temperature difference measurements are listed in Table 1.

Figure 2 shows a simplified diagram illustrating the execution of the FDI methodology in the MITR-II. Inputs to the computer program are the error bounds and the process variables such as secondary coolant and ambient temperatures which are not sensed at every sampling period. The error bounds need not be fixed. If necessary, they can be dynamically adjusted in the computer algorithm.

No false alarms were reported for continuous operation during the weekdays, extended over a period of several months. (MITR-II is started and shut down every week.) To demonstrate the fault isolation capabilities of this methodology, failures corresponding to errors in excess of the specified error were simulated while the reactor was in operation (with prior permission from the reactor safety committee). Typical cases are reported below.

1) Faulty sensor calibration. In a given measurement, bias was introduced in the conversion process from volts to engineering units. The alarm signal was received for the

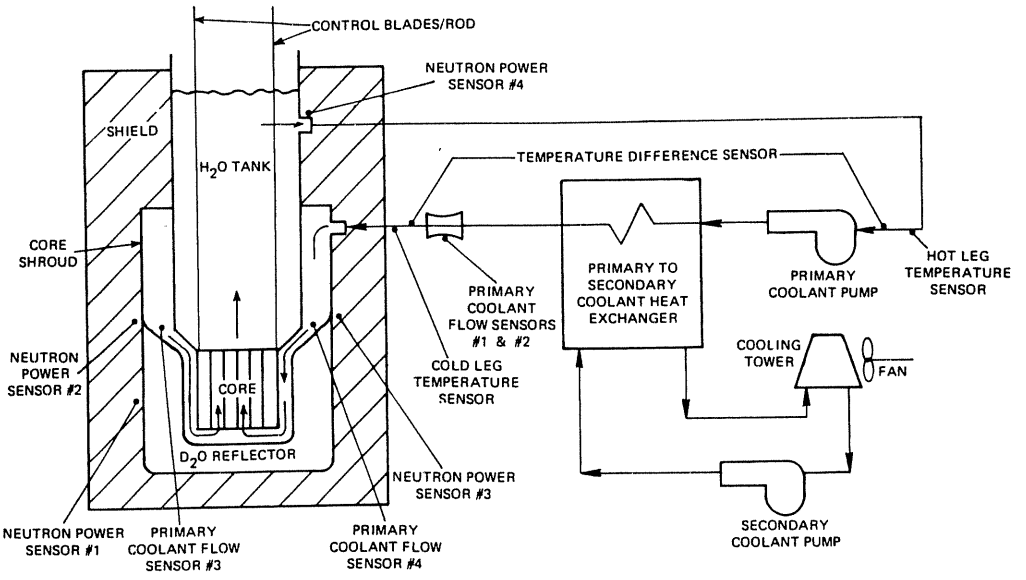

Fig. 1 Simplified schematic diagram for the nuclear reactor.

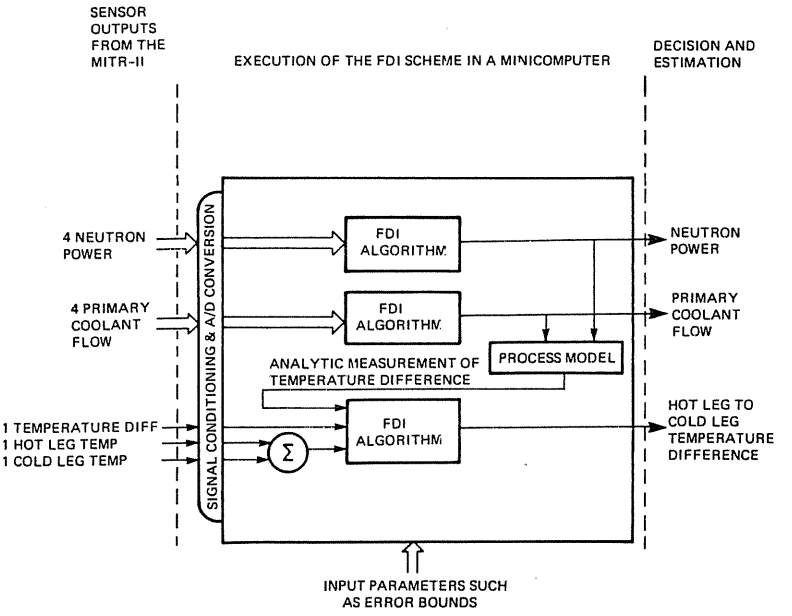

Fig. 2 Fault isolation and measurement validation scheme.

Table 1 Nominal values and error bounds of the process variables

Process variable	Nominal value	Error bound Steady-state	Transient
Neutron power, MW	4.8	0.25	0.5
Primary coolant flow, kg/s	143.0	10.0	10.0
Hot-leg to cold-leg temperature difference, °C	7.8	0.5	0.8

specific measurement and the validated estimate was automatically obtained from the remaining measurements.

2) Gradual drift. Drift was introduced in a given sensor output in the form of a ramp function. The alarm signal was received when the drift exceeded the permissible error bounds.

3) Degraded instrumentation. Instead of injecting random noise into the sensor outputs, the error bounds for the respective process variables were appropriately reduced. This action resulted in alarms signifying the simulation of erroneous instrumentation.

4) Failed sensor. Some of the sensors were disconnected from the data acquisition system. Immediately the respective sensors were identified as faulty.

5) Abnormal operation. As a means of extracting radiation for experiments, the MITR-II contains a port through the D_2O reflector. When this port is opened, due to changes in neutron distribution, scale factor for one of the neutron flux sensors was significantly altered, thus causing an alarm for faults. In this case, a validated estimate of neutron power was calculated as an average of the remaining three sensor outputs. The operator is thus alerted to the possibility that the port may have inadvertently been left open.

Summary and Conclusions

This paper presents a novel methodology for on-line fault detection and isolation (FDI) using all available information for direct and analytic sources. The methodology provides a fast and versatile algorithm that can be implemented in real time by a minicomputer. Only a minimal knowledge of sensor and plant noise statistics is required for application to physical processes.

The algorithm has been computer coded and verified by on-line demonstration in an operating nuclear reactor. A preliminary version of this algorithm was used for simulation of signal validation in powerplants. This FDI technique can be applied to fossil powerplants and chemical industries as well.

Appendix A

Development of the FDI Methodology

The redundant data can be modeled by the measurement equation

$$m = Hx + \epsilon \tag{A1}$$

where m is the $\ell \times 1$ measurement vector whose elements are obtained from either direct or analytic sources, H the $\ell \times n$ measurement matrix of rank n, x the $n \times 1$ true value of the measured variable, ϵ the $\ell \times 1$ noise or measurement error vector, and b the given symmetric error bound for all measurements, such that $|\epsilon_i| \leq b$ for $i = 1,2,\ldots,\ell$.

The measurements m can be combined to yield a set of linearly independent parity equations[3] given by

$$p = Vm \tag{A2}$$

where p is the $(\ell - n)$-dimensional parity vector and the projection matrix V has the following properties[3]:

$$VH = 0 \tag{A3}$$

$$VV^T = I_{\ell - n}, \text{ i.e., the rows of } V \text{ are orthonormal} \tag{A4}$$

and, from above, it follows that

$$V^T V = I_\ell - H(H^T H)^{-1} H^T \tag{A5}$$

Combining Eqs. (A1-A3) yields

$$p = V\epsilon \tag{A6}$$

i.e., the parity equations are independent of the true value x and contain the effect of measurement errors, including those that may result from a failure. In effect, the matrix V projects m on the $(\ell - n)$-dimensional subspace which is orthogonal to H. Thus, variations in the underlying measured variable x

which may obscure the failures are eliminated and only the inconsistencies among the measurements appear in the parity vector. Moreover, in the parity space, the columns of V define the ℓ distinct failure directions associated with each of the measurements. For example, if the ith measurement fails, the ith element of the ϵ vector grows. Then the ith column of V determines the direction along which p lies if $\epsilon = e_i$, where e_i is a column vector of zeros except for its ith element.

It can further be shown, using Eqs. (A4) and (A5), that an ℓ-dimensional residual vector $\eta = m - H\hat{x}$ where $\hat{x} = (H^T H)^{-1} H^T m$ is the least-squares-fit estimate of x and is related to parity vector p as

$$\eta = V^T p \tag{A7}$$

and

$$\eta^T \eta = p^T p \tag{A8}$$

For powerplant applications, the measured variables are not vector quantities. Rather the scalar process variables such as power, flow, temperature, pressure, etc., are of interest, i.e., $n=1$ and x is a scalar in Eq. (A1). Therefore, only scalar measurements will be considered in this paper. The measurement matrix can then be expressed, without loss of generality, as $H=[1,1,\ldots,1]^T$. Thus, using Eqs. (A2) and (A5-A7), the residuals can be derived as

$$\eta_i = m_i - \frac{1}{\ell}\sum_{j=1}^{\ell} m_j = \epsilon_i - \frac{1}{\ell}\sum_{j=1}^{\ell}\epsilon_j, \qquad i=1,2,\ldots,\ell \tag{A9}$$

i.e., the residual η_i is the difference between the ith measurement and the average of all the redundant measurements. Further, the component p_i of the parity vector p along the ith failure direction in the parity space is the scalar product of p and the unit vector $v_i/|v_i|$, where v_i is the ith column of the matrix V. Thus,

$$p_i = (v_i^T p)/|v_i| = \eta_i/|v_i|$$

by Eq. (A7). From Eq. (A5), $v_i^T v_i = (\ell-1)/\ell$ for the given H. Therefore, a simple relationship exists between the parity vector and the residual vector

$$p_i = \sqrt{\ell/(\ell-1)}\,\eta_i, \qquad i=1,2,\ldots,\ell \tag{A10}$$

Equation (A10) will be a useful relationship in deriving a computationally efficient method of identifying failures.

For normal operations, when no sensors have failed, the parity vector is small, which reflects the acceptable errors in all measurements that are mutually consistent within allowable error bounds. Following the corollary to the theorem in Appendix B, a set of ℓ measurements is defined to be consistent if the inequality

$$|p|^2 \le \theta^\ell = \begin{cases} \ell b^2 & \text{if } \ell \text{ is even} \\ \left(\dfrac{\ell^2-1}{\ell}\right) b^2 & \text{if } \ell \text{ is odd} \end{cases} \tag{A11}$$

is satisfied; otherwise, the set is defined to be inconsistent. The definition can be modified for unequal error bounds for individual measurements. In that case, evaluation of θ_ℓ in Eq. (A11) requires larger computations, as is evident from the theorem in Appendix B.

If a failure occurs, the set of measurements exhibits inconsistency and the parity vector grows in magnitude in a direction unique to the failed measurement. The increase in magnitude signifies detection of a failure, and the failed measurement may be identified from the direction of growth of the parity vector. Daly et al.[4] have shown that an FDI decision can be made on the twin basis of relative orientation and magnitude of the projection of the parity vector with respect to various subspaces spanned by one or more failure directions. An alternative approach is to make a decision solely on the basis of magnitudes of the projections of the parity vector on the ℓ distinct subspaces, each orthogonal to one of the ℓ failure directions. This approach proves to be less complex and computationally more efficient for scalar measurements, as seen below.

Let $S=\{m_1,m_2,\ldots,m_\ell\}$ be the set of measurements and S^i be a subset of $(\ell-1)$ measurements such that $m_i \notin S^i$. Let p^i be the projection of the $(\ell-1)$-dimensional parity vector on the $(\ell-2)$-dimensional subspace orthogonal to the failure direction corresponding to m_i. Then, Eqs. (A7), (A8), and (A10) can be combined to yield

$$|p^i|^2 = \sum_{j=1}^{\ell}\eta_j^2 - \frac{\ell}{\ell-1}\eta_i^2 \tag{A12}$$

Let $\bar{\eta}^i$ be the $(\ell-1)$-dimensional residual vector and $\bar{p}^i$ the corresponding $(\ell-2)$-dimensional parity vector generated from all measurements in S^i where $m_i \notin S^i$. Then,

$$|\bar{p}^i|^2 = \sum_{\substack{j=1 \\ j\neq i}}^{\ell} (\bar{\eta}_j^i)^2 \tag{A13}$$

where

$$\bar{\eta}_j^i = \epsilon_j - \frac{1}{\ell-1}\sum_{\substack{k=1 \\ k\neq i}}^{\ell}\epsilon_k \text{ for every } j\neq i$$

Using Eqs. (A8), (A9), (A12), and (A13), it can be shown that $|\bar{p}^i| = |p^i|$, i.e., the magnitude of the parity vector generated from all $(\ell-1)$ measurements in S^i is identically equal to the magnitude of the projection of the parity vector generated from all ℓ measurements in S on the subspace orthogonal to the ith failure direction. Therefore, for any ℓ measurements where $\ell>2$, $|\bar{p}^i|$ can be obtained from the residuals η using Eq. (A12) without recalculating $\bar{\eta}^i$ for the subsets S^i, $i=1,2,\ldots,\ell$. Following the definition in Eq. (A11), if $|p^i|^2 \le \theta^{\ell-1}$, then the subset S^i is consistent; i.e., none of the $(\ell-1)$ measurements in S^i have exceeded the error bound b—otherwise, at least one of these $(\ell-1)$ measurements is not functioning normally.

Formulation of the FDI Algorithm

The FDI algorithm is formulated on the basis of relative consistencies of appropriate subsets of the full set of measurements. The consistency of any subset is determined by checking the magnitude of the respective parity vector which is identically equal to the magnitude of the residual vector. The largest consistent subset (if it exists) provides a validated estimate of the measured variable and the remaining measurements (if any) are isolated on the basis of large residuals. Figure A1 shows a flow chart of the algorithm. The basis and the computations involved in the algorithm are described below.

If the full set of ℓ measurements is consistent, all measurements are valid and estimate $\hat{x}$ is the average of all measurements; otherwise detection of failure(s) is implied and further computation is necessary for failure identification. The number N of inconsistent subsets S^i, $i=1,2,\ldots$, provides information for failure identification where S^i contains all measurements except m_i, as defined earlier.

1) If $N<(\ell-1)$, no measurement is identified as failed and the estimate $\hat{x}$ is obtained as the average of the N measurements m_i corresponding to the N inconsistent subsets S^i.

2) If $N=\ell-1$, the estimate $\hat{x}$ is obtained in the same way, but the measurement m_i not contained in the only one consistent subset S^i may be identified as failed; the failure is high if $m_i > \hat{x}$ and low if $m_i < \hat{x}$.

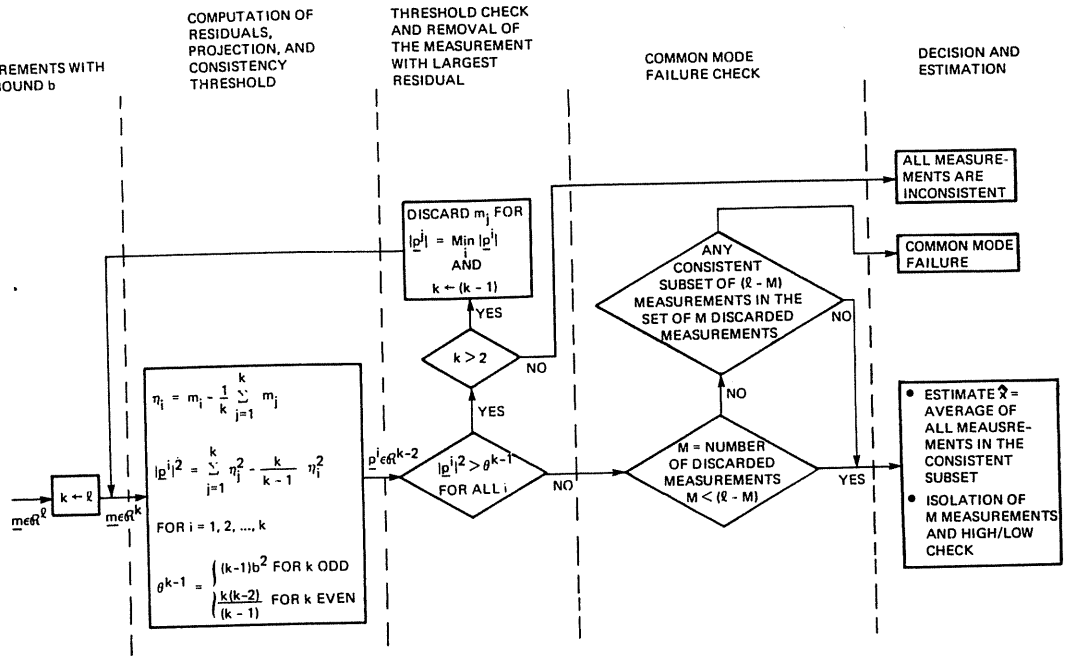

Fig. A1 Flow chart for the FDI algorithm.

3) If $N=\ell$, i.e., all subsets are inconsistent, more than one failure has occurred. In that case, the measurement m_i corresponding to the least inconsistent subset S^i, i.e., for which $|p^i|$ is the minimum or the residual $|\eta_i|$ is the largest, is most likely to have failed. Therefore the aforesaid measurement m_i is discarded and the subset S^i that does not contain m_i is considered. The steps are repeated until either the subset under consideration contains two measurements or any consistent subset has been located.

If no consistent subset exists, the measurements are mutually inconsistent and $\hat{x}$ cannot be obtained. On the other hand, if a consistent subset exists, the number of measurements in this subset is identically equal to $(\ell-M)$, where M is the total number of measurements discarded in the previous steps. If $(\ell-M)>M$, i.e., $M\leq[(\ell-1)/2]$, implying that the consistent subset contains more than half of all ℓ measurements, then $\hat{x}$ is computed and the M discarded measurements are isolated. If $(\ell-M)\leq M$, i.e., $M>[(\ell-1)/2]$, the consistency of any subset of $(\ell-M)$ measurements of the set of M discarded measurements implies a common-mode failure and $\hat{x}$ cannot be computed; otherwise, $\hat{x}$ is computed and the M discarded measurements are isolated. As a typical example, consider a set of four measurements, $\ell=4$. If two measurements fail identically, the failure can be detected as a common mode and $\hat{x}$ cannot be computed. On the other hand, if two measurements fail nonidentically, identification is possible even though the number of failures exceeds $[(\ell-1)/2]=1$. Thus if the number M of discarded measurements exceeds $[(\ell-1)/2]$ and this set of all discarded measurements contains one or more consistent subsets of $(\ell-M)$ measurements, then there are two or more consistent subsets of $(\ell-M)$ measurements in S that are mutually inconsistent, which implies a common-mode failure; otherwise, the failed measurements can be isolated.

A preliminary version of the algorithm, limited to five measurements, was applied to simulation of signal validation in powerplants.[5] The algorithm presented above is more efficient, compact, and versatile than its earlier version and is applicable to any number of measurements.

Limitations

The limitations of the algorithm, in its present form, are:

1) Sufficient information on tolerances, calibration, nonlinearities, etc., for the measurements must be available for determination of error bounds. (Such information is usually available from the specifications of instrument manufacturers.)

2) For a given process variable, all measurements are constrained to have equal error bounds. (The algorithm can be modified to eliminate this limitation.)

3) Since the algorithm seeks out the largest consistent subset of measurements, the FDI decision could be invalid if more than half of the total measurements fail identically.

Geometric Representation of the FDI Methodology

A simple geometric representation of the FDI methodology for a set of three scalar measurements m_1, m_2, and m_3 with respective errors ϵ_1, ϵ_2, and ϵ_3 is given in Fig. A2 for illustration. The allowable error regions for three subsets, each containing two measurements, are shown in Fig. A2a. Each region is an infinite prism of a square cross section with its axis along the direction of the measurement which is not contained in the respective subset, and is seen to be divided into three regions. The region centered around the origin is a cube of side 2b representing the allowable error region for measurements m_1, m_2, and m_3 and is shared by all three prisms. The other two semi-infinite regions in a prism on either side of the cube represent the failure region for the third measurement not included in the pair associated with the prism.

Figure A2b shows the projection of the allowable error regions of different sets of measurements on the parity space which is a plane orthogonal to the direction $[1, 1, 1]^T$ in the three-dimensional measurement space. Projection in this plane is chosen because changes in x, the measured variable, do not appear in the plane. The three infinite prisms are projected as three infinite strips centered along the three failure directions. The parity space is then divided into several regions, each of which is associated with the decisions of the FDI algorithm. The hexagonal region, surrounding the origin, is the intersection of the three infinite strips and is also the projection of the error cube. The two corners (b, b, b) and $(-b, -b, -b)$ of the cube are projected on the origin, and the remaining six corners of the cube correspond to the six corners of the hexagon. Within the hexagon, all three measurements are considered to be valid and the estimate is

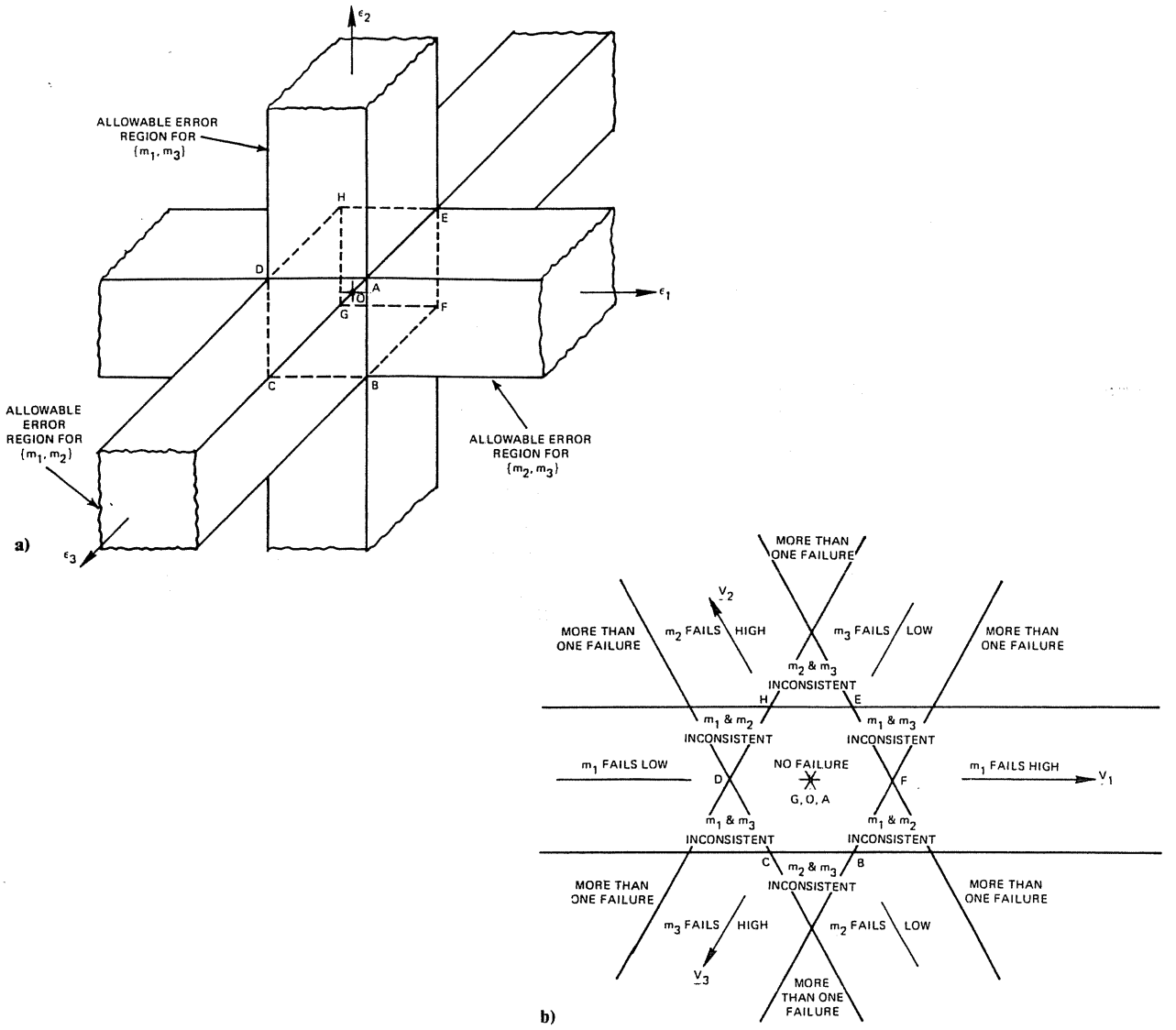

Fig. A2 a) Allowable error regions in the measurement space. b) Allowable error and decision regions in the parity space.

$\hat{x}=(m_1+m_2+m_3)/3$. The six triangles on the six sides of the hexagon represent the regions of intersection of any two strips that lie outside the remaining third strip and represent the cases of one inconsistent and two consistent subsets; the measurement not contained in the inconsistent subset is the best choice for obtaining the estimate. For example, in the region marked "m_1 and m_3 inconsistent," $|m_1-m_3|>2b$ and $\hat{x}=m_2$. The six semi-infinite regions in the strips adjacent to the hexagon indicate the failure of one specific measurement. For example, if the parity vector is confined in the region marked "m_1 fails high," the subsets $\{m_1, m_2\}$ and $\{m_1, m_3\}$ are inconsistent and the subset $\{m_2, m_3\}$ is consistent; therefore, $x=(m_2+m_3)/2$ and $m_1>\hat{x}$ indicates a high failure. The remaining part of the parity space not covered by the three infinite strips consists of six semi-infinite forks. If all three subsets are inconsistent, the parity vector lies in any one of these forks and failure of more than one measurement is implied; thus, no estimate can be obtained.

Appendix B

Theorem: Let the mapping from R^ℓ to R^1 be defined as

$$f(x)=x^TCx \quad \text{for} \quad x\in E^\ell=\{x_i: |x_i|\le b_i\}$$

where

$$C=I_\ell-H(H^TH)^{-1}H^T$$

and

$$H^T=[1, 1,..., 1]$$

Then

$$\underset{x\in E^\ell}{\text{Max}} f(x)=\sum_{i=1}^{\ell} b_i^2-\frac{1}{\ell}\underset{\xi_i}{\text{Min}}\left(\sum_{i=1}^{\ell}\xi_i b_i\right)^2$$

where ξ_i can be either 1 or -1.

Proof: Since

$$f(x)=x^TCx=\sum_{i=1}^{\ell}x_i^2-(1/\ell)\left(\sum_{i=1}^{\ell}x_i\right)^2$$

$$=\sum_{i=1}^{\ell}\left(x_i-(1/\ell)\sum_{j=1}^{\ell}x_j\right)^2\ge 0$$

everywhere in E^ℓ, C is positive semidefinite. Therefore, f is a continuous convex mapping.[7] Furthermore, since E^ℓ is compact, maximum of f occurs on the boundary of E^ℓ. Continuing in this way, it can be argued that maximum occurs

at one of the corners, $\{x_1, \ldots, x_\ell: x_i = \pm b_i\}$ of E^ℓ. Proof is thus complete.

Corollary: If $b_i = b$ for every i, then

$$\text{Max} f(x) = \begin{cases} \ell b^2 & \text{for } \ell \text{ even} \\ [\ell - (1/\ell)]\, b^2 & \text{for } \ell \text{ odd} \end{cases}$$

Proof: Noting that $f(x)$ is invariant under permutation of x_i,

$$\text{Max} f(x) = \{\ell - (1/\ell)\,[n - (\ell - n)]^2\} b^2$$

$$= 4\ell(n/\ell)\,[1 - (n/\ell)]\, b^2$$

where

$$x_i = \begin{cases} b & \text{for } i = 1, 2, \ldots, n \\ -b & \text{for } i = n+1, \ldots, \ell \end{cases}$$

A function $\phi(\theta) = \theta(1-\theta)$ attains the maximum at $\theta = \frac{1}{2}$ in the domain $\theta \in [0,1]$. However, $(n/\ell) \in [0,1]$ can have only $(\ell + 1)$ discrete values. Therefore, $f(x)$ attains a maximum at

$$n = \begin{cases} \ell/2 & \text{if } \ell \text{ even} \\ (\ell-1)/2 \text{ or } (\ell+1)/2 & \text{if } \ell \text{ odd} \end{cases}$$

The proof follows immediately.

Acknowledgments

The authors acknowledge the benefits of discussion with Dr. J.E. Potter and Dr. E. Fogel. The many helpful suggestions from D.K. Pike and the cooperation of Prof. David Lanning, John Bernard, Paul Menadier, and other personnel of the MIT Nuclear Reactor Laboratory during the experimentation phase are greatly appreciated. This work was supported by the IR&D funds of The Charles Stark Draper Laboratory, Inc.

References

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

[2] Desai, M.N., Deckert, J.C., and Deyst, J.J., "Dual Sensor Failure Identification Using Analytic Redundancy," *Journal of Guidance and Control,* Vol. 2, May-June 1979, pp. 213-220.

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

[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, Jan.-Feb. 1979, pp. 9-17.

[5] "On-line Power Plant Signal Validation Technique," Electronic Power Research Institute, Palo Alto, Calif., Rept. EPRI NP-2110, Nov. 1981.

[6] "Reactor Systems Manual," Nuclear Reactor Laboratory, Massachusetts Institute of Technology, Cambridge, Mass., Rept. MITNRL-004, 1980.

[7] Rudin, W., *Principles of Mathematical Analysis,* Vol. I, McGraw-Hill Book Co., New York, 1976.