NSC-91

Fifteenth National Systems Conference
Roorkee, March 13-15, 1992

Knowledge Based Sensor Failure Management Using Observers

C. V. Srinatha Sastry, B. Satyabhagavan, J.R. Raol
National Aeronautical Laboratory, Bangalore

N.K. Sinha
MC Master University, Canada

ABSTRACT

An expert system was developed for sensor failure management for control systems. Keeping the basic structure intact, the expert system can be used in real time environment with suitable modifications. A new strategy has been presented which is useful to investigate in situations with many alternatives. providing almost immediate solutions for corrective measures.

1. INTRODUCTION

Some of the realistic problems in control systems which are complex and subject to failures in the connected measuring instruments (sensors) require almost instantaneous solutions for the dynamic systems to hsve the desired performance. When a sensor fails,there is a need to replace the failed sensor by a redundant sensor for the purpose of failure management; Mathmatical modelling and computer simulation of control problems provide useful solutions by which real time sensor failure management control systems can be designed using minimum human intervention. The computer software, written for this purpose in conventional, procedure oriented languages when implemented are time consuming and hence inefficient for on-line failure management systems. Methods of artificial intelligence are more effective resulting in qualitative decisions by heuristic reasoning in complex situations.

Keeping the above facts in view, a knowledge based simulation software for failure management purposes, was developed. This expert system is an interface of several TURBO-C and TURBO-PROLOG modules which can be linked and executed in real time on PC. The expert System consists of 1) simulation of sensor outputs, 2) observer computations and 3) sensor failure, management.Figure 1 shows the block structure of the expert system.

2. REDUNDANT SENSOR PACKAGES

Accuracy in sensor output is an important aspect in a feedback control system. Failure in one or more sensors resulting in faulty feed-back signals can produce abnormal changes in the dynamic performance of the system. One of the methods adopted to take care of such critical situations is to provide multiple sensors for each signal Dath. resulting in redundant measurements. If failure occurs in a sensor and is detected, it can be disconnected and its counterpart in the redundan't sensor package can be relied upon for the feedback signal. It is assumed here that all those redundant sensors in different sensor packages, which are used to measure the same signal do not fail together. One of the methods adopted to detect sensor failure is to have a triplex sensor package system and compare the three measured values. from similar sensor types for equality.
However, analytical treatement of the control problems provides some techniques by which the above type of multiple (more than two) hardware redundancy can be replaced by only one pair of redundant Sensor packages[3]. This will provide computational procedures for easy detection, diagnosis and selection of the proper sensor to get the correct output.

3. ESTIMATION USING OBSERVERS

The development of a failure management expert system is tried for a linear second order aircraft system with a single control input. The state vector X has the components α (angle of attach) and q (pitch rate) which are measured simultaneously by two sets of sensors providing pairs of identical values (provided none of them fail) represented by

Y11 and Y12 (sensor type 1)
and Y21 and Y22 (sensor type 2).

Under no-fail conditions, it is obvious that

$$Y11 = Y12 \quad \text{and} \quad Y21 = Y22 .$$

As already stated, for sensor failure management purposes, apart from the sensor package (measuring two outputs) and its counter part. analytical design of observers[4] to estimate correct values of the output signals is also' considered'. We have one observer for each sensor (Fig.2). Each observer driven by one of the' two outputs of a package estimates the other output. Thus the sensor outputs and their estimates through observers provide the redundancy for comparison purposes.

The two sets of observer outputs resulting from the analytical scheme to estimate the desired values for the output signals can be represented by :

Yllh and Y12h (redundancy for sensor type 1)
Y21h and Y22h (redundancy for sensor type 2)

If all sensors are good and if the dynamic parameters of the system are known perfectly, then all observer estimates will converge to sensor measured values. In the event of the failure of one of the sensors, observer estimates of the other output, driven by the failed sensor output will be in error. These along with other sensor and observer outputs are used to evolve an elegant scheme for detection and diagnosis of sensor failure. When a sensor is detected as failed, it is switched off and its output signal is replaced by the output of the corresponding sensor of the same sensor type belonging to the other sensor package. As already stated, design and computation of observer equations involve numerical computational procedures.

4. ESTIMATION OF THRESHOLD VALUES

If the mathematical model of the system is accurate enough and sensors operate normally, observer states converge quickly to outputs from sensors. Thus differences betneen observer outputs and sensor outputs (observer residuals) will be very small, oscillating around desired values with a certain maximum deviation. This maximum residual is the design threshold. This can be estimated analytically for each sensor.

Fig.3 represents the block diagram to compute threshold values. Figures 4 & 5 show quick convergence of observer outputs, corresponding residuals and threshold values.

If failures have occured in one or more sensors, there will be large deviations in observer outputs resulting in large observer residuals exceeding the corresponding threshold value. Analysis of these sensor and observer outputs and observer residuals is the essence of sensor failure management scheme which uses knowledge base and methods of artificial intelligence.

5. SENSOR FAILURE MANAGEMENT THROUGH KNOWLEDGE-BASED SYSTEMS

It is already stated in introduction that knowledge-based symbolic reasoning detects significant abnormalities in sensors, pinpoints the failed sensor or sensors and discards the failed sensor(s). A rule-based approach is adopted to detect the defective sensor. The inference engine makes such decisions at each step based on

(1) the current sensor and observer output status which is provided by the information pre-processing software written in a procedure oriented language; and

(2) the knowledge stored in the knowledge base

5.1 FORMATION OF FAILURE INDICATOR VECTORS

At any point of time, under no-fail conditions, observer outputs converge to the corresponding sensor outputs, which means that each of the resultant observer residuals is less than the corresponding threshold value. Due to existance of more than one sensor types and their redundancy and the corresponding observers, several such absolute differences and hence several threshold bound conditions can be obtained. However, it is a finite set of absolute differences. with the number of elements of the set depending on the number of sensor types and packages. If fault occurs in a sensor, some of the absolute differences involving the erroneous values (in sensor and observer outputs)exceed the correspondin; threshold values while the remaining differences (corresponding to outputs from fault-free sensors) continue to be less than the threshold values. Hence there exists only two conditions snd each one of these threshold bound and threshold unbound conditions can be represented by one of the two arbitrarily selected symbols. Thus the absolute differences and the corresponding symbols form tuo ordered sets having a one-to-one correspondance among themselves.

Under no-fail conditions, the symbol set consists of only one symbol which corresponds to the threshold bound condition and repeats as many time5 as the number of absolute differences occur.

Consider all the conditions where only one of the sensor fails, with the remaining sensors in good condition (single sensor failure conditions). When failure occurs in a sensor, some of the absolute differences are threshold bound and the remaining are threshold unbound. Hence the symbol set consists of both the symbols, with the repetition of the tno symbols. The number of times a symbol repeats (symbol repetition factor) is the same as the number of threshold bound or threshold unbound conditions it represents. By the same procedure, any other single sensor failure condition will result in a symbol set with different ordering of the same tno symbols. Redundancy in sensors, similarity in observer constructions and the same procedures adopted for the computations of the residuals in all single sensor failure conditions results in the property that the symbol repetition factors continue to have the same values in all the above cases,even though the ordering is different for different cases. Thus we have a specific vector of tuo symbolic elements for the failure of a specific sensor, called failure indicator vector. This means that there exists a unique pattern of symbols (failure indicator vector) for each sensor under single sensor failure conditions.

Similarly, unique patterns of symbols (failure indicator vectors) can be derived in cases of two sensors failing simultaneously (double sensor failure conditional. As before, symbol repetition factors for the two symbols are same in all cases of double sensor failure conditions, but are different from the ones obtained .in single sensor failure conditions. It is important to note that the absolute difference of two values will be threshold bound or unbound depending on whether both the values are almost same or one of them is in error. If both the values used for computing an absolute difference are in error, nothing can be said about their abosolute difference. Such absolute differences whose behaviour cannot be predicted should not be considered in generating failure indicator vectors.

Thus at any point of time, a unique failure indicator vector can be generated which forms the input for the inference engine to act on the knowledge base for sensor failure management. The knowledge base itself consists of fixed ordered symbol vectors for single sensor failure and double sensor failure conditions.

Appendix I illustrates the procedure for sensor failure vector generation for all. possible cases for a second order system and the standard failure indicator vectors.

5.2 LOGIC FOR SENSOR FAILURE MANAGEMENT

The knowledge base consists of facts and rules pertaining to single and double sensor failure conditions. The facts consist of standard failure indicator vectors whose elements are the same symbols which are chosen to generate failure indicator vectors.The patterns and properties of the generated failure indicator vectors form the basis to create standared indicator vectors to be used in the facts in the knowledge base. The'standard failure indicator vector for a particular type of failure may be formed by grouping together the two symbols depending on the corresponding symbol repetition factors. When failure occurs, the generated failure indicator vector uill have the same symbols uith same repetition factors as compared .to the corresponding standard failure indicator vector, but the elements are arranged in a different (unique) order. Reordering is done in the generated failure indicator vector grouping the two symbols together to match uith the standard failure indicator vector. The reordering sequence uhich is again unique in case of a failure, will decide the failure of a particular sensor (Tables 1 and 2).

During real time decision making process,the inference engine starts uith rules which test the double sensor failure conditions. The rule acquires the failure indicator vector generated in the procedure oriented software. This vector undergoes suitable reordering before the rule uses the fact containing the appropriate standard failure indicator vector for pattern matching purposes to detect and diagnose the failure in pairs of sensors.

Consider the case of two sensors failing at different instances of time. resulting in single sensor failure condition for some time and simultaneous failure of two sensors for a different period of time.The software takes care of such situations by switching over the logics for single and double sensor failure conditions whenever it is needed.

With this procedure which pin points a failed sensor or pair of sensors, the software returns a flag, which is used in the reconfiguration procedure. Reconfiguration is done by replacing the failed sonsor output by the corresponding sensor output, depending on the value of the flag.

6. RESULTS AND DISCUSSIONS

As already discussed, the techniques of detection and diagnosis to identify a failed sensor is a single step ,procedure in this expert system. due to the uniqueness property of the generated failure indicator vector in respect of the failed sensor.

The results show that under no fail' Conditions, residuals always remain threshold bound, which means that observer outputs are almost equal.to sensor outputs. Figures 4 and 5 show these small differences between sensor and observer outputs and also convergence of residuals uith a maximum value, in,respect of the two sensor types.

Failure signals of different magnitudes are chosen to simulate failure in differenat sensors. Each one of these is a deviation pulse function and the appropriate failure signal is added to the four sensor outputs uith a multiplication factor. Depending on the choice of 0 or 1 for the multiplication factor a sensor will be deemed as normal or failed. Under double or single sensor failure condition, the inference engine returns a flag. The output from the failed sensor· is replaced by that of corresponding redundant sensor depending on the value of the flag.

Figure 6 shows the sensor ST11 which has failed after a certain stage. Since Y11 is in error, output Y21h of the observer driven by Y11 is also in error. Hence the corresponding'residuals res11 and res21 are threshold unbound.

However. :he output Y11h of the observer driven by sensor output Y21 is not in error. Hence Y11h is equal to Y12h. figure 7 show reconfiguration in which the sensor ST11 is replaced by ST12 after failure is detected, uith a maximum residual value greater than threshold limit at that moment. Similar results were obtained in all cases of double sensor failure conditions.

7. CONCLUSIONS

The kxpert system which has been developed by interfacing many modules in Turbo-C and Turbo-PROLOG, is found to be very effective in terms of programming efficiency and simple procedure for logical reasoning. Keeping the basic structure intact, the expert system can be used in a real time environment with suitable modifications. It is easy to enhance the knowledge base for searching various

alternatives. The failure management scheme for a second order system considered in this paper has two rules with each rule having several alternatives, with a scope for expansion.
Generating failure indicator vectors permits use of efficient pattern matching technique available in PROLOG to detect and localize simulated failures as a single step procedure. The scheme applied here may also be extended to higher order systems with more outputs. To avoid complexity in generating higher dimentional failure indicator vectors, each sensor packge may be considered to consist of subpackges with a *set of* two of the sensors. The tasks in sensor failure management can thus be accomplished with little changes in the knowledge base.

8. ACKNOWLEDGEMENT

The authors would like to thank Director, NAL and Head, FMCD for their support in carrying out this work.

REFERENCES

1. R.N. Clark, D.C. Fosth. V.M. Walton
   Detecting Instrument Malfunction in Control Systems IEEE Transactions on Aerospace / Electronic Systems
   Vol AES-11 No.4 July 1975 pp 465-473
2. David A. Handleman and Robert F. Stengel
   Combining Expert System and Analytical Redundancy Concepts for Fault-Tolerant Flight Control
   Journal of Guidance Vol.12 No.1,Jan-Feb '89
3. J.R.Raol, G.Girija, V.Parameswaran
   A Sensor failure detection schede using analytical redundancy and U-D filtering algorithm for LCA. NAL Project Document FC 9006 March 1990, restricted
4. C.V.Srinatha Sastry, B.Satyabhagavan, J.R.Raol, N.K.Sinha. A scheme for sensor failure management using observers and knowledge based approach
   NAL Project Document FC 9009 July 1990
5. Thomas Kailath
   Linear Systems , Prentice-Hall,USA 1980
6. TURBO PROLOG USER'S GUIDE (sion 2
   Borland International
7. TURBO - C USER'S GUIDE (veraion 2.0)
   Borland International

APPENDIX I

FIRST ORDER OBSERVER FOR A 2nd ORDER SYSTEM

Consider the following equations

$$x1 = a11*x1 \;\; t \;\; a12*x2 \;\; t \;\; b1*u$$

$$\dot{x}2 = a21*x1 \;\; t \;\; a22*x2 \;\; + \;\; b2*u$$

and $y = x2$

To design observer for **xl** (to calculate $\hat{x}1$):

Define $y1 = y - a22*y - b2*u = a21*x1$

Observer: $\hat{x}1 = a11*\hat{x}1 + a12*y + b1*u \;\; t$
$$11*(y1 - a21*x1) \qquad ....(1)$$

Define $\tilde{x}1 = x1 - \hat{x}1$ observation **error** (residual),

and $\tilde{x}1(o) = x1(o) - \hat{x}1(o).$

$$\tilde{x}1 = \dot{x}1 - \hat{x}1 = (a11 - 11 * a21)*\tilde{x}1$$

$$\tilde{x}1(t) = \tilde{x}1(o)*e^{-(a11 - 11 * a21)t}$$

By proper choice of 11 (convergence coefficient), error x1(t) may be made to decay fast.

Define Convergence Factor = all - 11 * a21.
Convergence Coefficient 11 is computed by taking a, sufficiently large value for. the converaence factor.

Equation (1) can *be* urittm as

$$\dot{\theta}(t) = (a11 - 11*a21) \;\; t \;\; (a12 - 11*a22 + 11(a11-12*a21))y \;\; t \;\; (b1-11*b2)*u \quad ...(2)$$

and

$$x1 = \theta \;\; t \;\; 11*y \qquad ...(3)$$

where

$$Y = x2.$$

Equation (2) is solved for θ by **a** numerical method. $\hat{x}1$ is obtained by substituting θ in(3).

Similarly, we can design the observer for x2 (computation of $\hat{x}2$) by choosing a suitable convergence factor.

APPENDIX II

FAILURE INDICATOR VECTOR FOR 2nd ORDER SYSTEM

Figure 2 illustrates **a** dynamic system with duplex sensor packages and corresponding observers. Each of the sensor outputs represented by

Y11, Y21, Y12 and **Y22**

drives an observer resulting in observer outputs represented by

Y21h, Y11h, Y22h and Y12h.

If all the sensors are good then,

$$Y11 = Y12 = Y11h = Y12h \qquad ...(1)$$

and
$$Y21 = Y22 = Y21h = Y22h \qquad ...(2)$$

These equality relations correspond to the two sensor types measuring the two states of **the** dynamic system. Due to the observer threshold values E1 and **82** corresponding to the two sensor types, the quantities in the equality relations (1) and (2) are not exactly **equal** but their absolute differences taken in pairs are bound by the threshold values.

Thus, the above equality relations reduce *to* two sets of six inequalities (each set corresponding **to** a sensor type) as follows:

Set 1	Set 2
$\lvert Y11 - Y12 \rvert - E1 \leq 0$	$\lvert Y21 - Y22 \rvert - EZ \leq 0$
$\lvert Y11 - Y11h \rvert - E1 \leq 0$	$\lvert Y21 - Y21h \rvert - E2 \leq 0$
$\lvert Y11 - Y12h \rvert - E1 \leq 0$	$\lvert Y21 - Y22h \rvert - E2 \leq 0$
$\lvert Y12 - Y11h \rvert - E1 \leq 0$	$\lvert Y22 - Y21h \rvert - E2 \leq 0$
$\lvert Y12 - Y12h \rvert - E1 \leq 0$	$\lvert Y22 - Y22h \rvert - E2 \leq 0$
$\lvert Y11h - Y12h \rvert - E1 \leq 0$	$\lvert Y21h - Y22h \rvert - E2 \leq 0$

Representing the quantities in the LHS of thene two sets of inequalities by d1, d2, d3, d4, d5 and d6 and e1, e2, e3. e4, e5 and e6 respectively, we have.

$d_i \leq 0$ and $e_i \leq 0$ $(i = 1, \ldots, 61$
for no-failure condition.
If the sensor ST11 is bad, its output Y11 and hence the corresponding observer output Y21h are in **error.** This results in some of the absolute differences (involving the erroneous values Y11 and Y21h) exceeding the threshold values. Therefore,

$d1 > 0$, $d2 > 0$, $d3 > 0$ but $d4 \leq 0$, $d5 \leq 0$, $d6 \leq 0$ and
$e1 \leq 0$, $e3 \leq 0$, $e5 \leq 0$ but $e2 > 0$, $e4 > 0$, $e6 > 0$

Further, the conditions of 'less than' and 'greater than' can be represented by two symbols say '0' and '1' respectively. With this representation, when sensor ST11 alone fails, the vector of differences

{d1, d2, d3, d4. d5, d6, e1, e2, e3, e4, e5, e6}

will have a one-to-one carrespondance with

{ , 1 , 1 , 0 , 0 , 0 , 0 , 1 , 0 , 1 , 0 , 1}

This is 'generated failure indicator vector'. Fable 1 gives the generated failure indicator vectors in respect of all single sensor failure conditions.

Consider the chse of two sensors ST11 and ST21 failing together. The sensor and observer outputs corresponding to these are:

Y11, Y21 and Y21h, Y11h

all of the *four* being in error. As before, the absolute differences forming the failure indicator vector are either threshold bound or threshold unbound. But, it is important to note that nothing can be said about the absolute differences

$\lvert Y11 - Y11h \rvert$ and $\lvert Y21 - Y21h \rvert$

as they may be threshold bound or unbound. This .is because, both the values involved in these differences are in error. Hence, the inequality relations involving these two absolute differences will have to be ignored resulting in the failure indicator vector having less number of elements, compared to single sensor failure conditions.

Table 2 gives the failure indicator vectors in respect of all double ***sensor*** failure conditions.

Table 1:Failure indicator vectors with symbol 0 and 1 for single sensor failure conditions

Sensors	d1	d2	d3	d4	d5	d6	e1	e2	e3	e4	e5	e6
ST11	1	1	1	0	0	0	0	1	0	1	0	1
ST21	0	1	0	1	0	1	1	1	1	0	0	0
ST12	1	0	0	1	1	0	0	0	1	0	1	1
ST22	0	0	1	Q	1	1	1	0	0	1	1	0

Standard failure indicator vector :

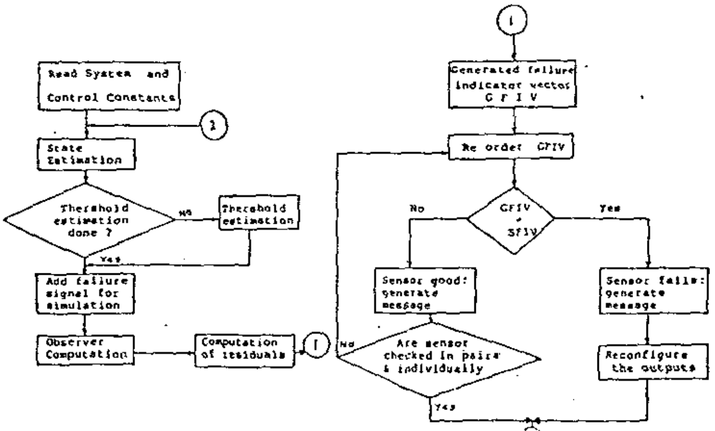
{1 1 1 1 1 1 0 0 0 0 0 0}

Table 2:Failure indicator vectors with symbol 0 and 1 for double sensor failure conditions

Sensors	d1	d2	d3	d4	d5	d6	e1	e2	e3	e4	e5	e6
ST11 & ST21	1	-	1	1	0	1	1	-	1	1	0	1
ST11 & ST22	1	1	-	0	1	1	1	1	0	-	1	1
ST21 & ST12	1	1	0	-	1	1	1	1	-	0	1	1
ST12 & ST22	1	0	1	1	-	1	1	0	1	1	-	1

Standard failure indicator vector :

{1 1 1 1 1 1 1 1 0 0}



Read System and Control Constants
1
State Estimation
Thershold estimation done ?
No
Thershold estimation
Yes
Add failure signal for simulation
Observer Computation
Computation of residuals
1
1
Generated failure indicator vector G F I V
Re order GFIV
GFIV = SFIV
No
Yes
Sensor good: generate message
Sensor fails: generate message
Are sensor checked in pairs & individually
No
Yes
Reconfigure the outputs
1

Fig. 1 Flow diagram for Expert system for sensor failure management (Note: GFIV = Generated failure indicator vector SFIV = standard failure indicator vector)

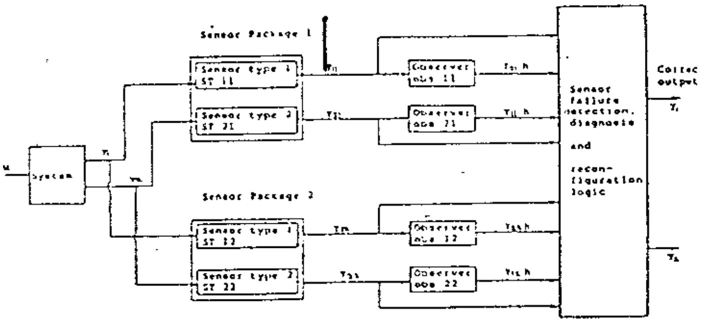


Fig.2 Block diagram [illegible] sensors and obser[illegible] for [illegible] outputs.

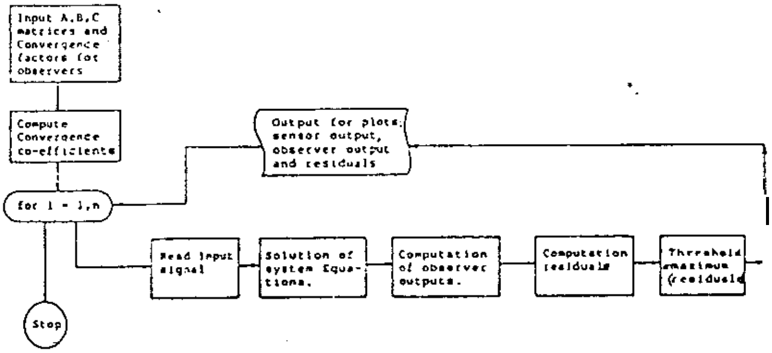

Input A,B,C matrices and Convergence factors for observers
Compute Convergence co-efficients
Output for plots: sensor output, observer output and residuals
for i = 1,n
Read input signal
Solution of system Equa-tions.
Computation of observer outputs.
Computation residuals
Threshold maximum (residuals)
Stop

Fig.3 Computation of threshold values

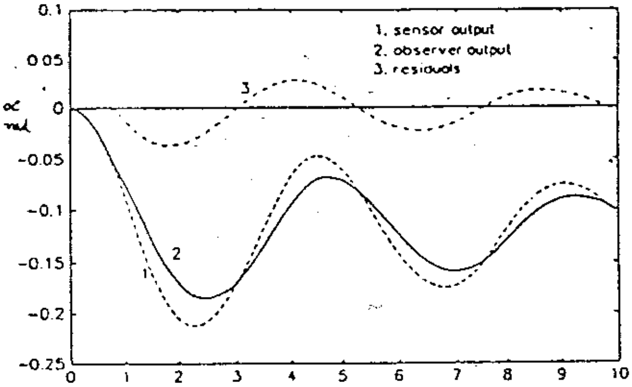


Fig 4. OBSERVER AND SENSOR OUTPUTS AND RESIDUALS FOR ST11 (NO FAILURE CONDITION)

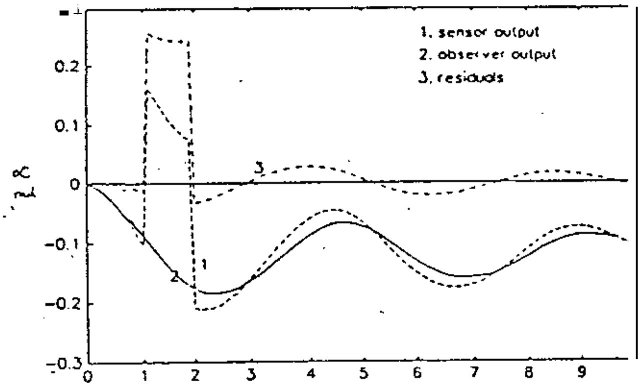


Fig 6. OBSERVER AND SENSOR OUTPUTS AND RESIDUALS FOR ST11 (FAILURE CONDITION)

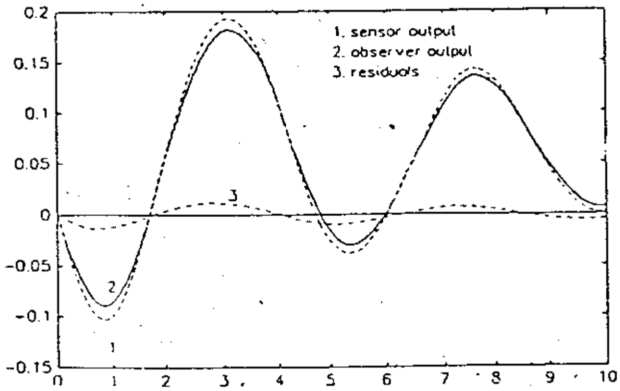


Fig 5. OBSERVER AND SENSOR OUTPUTS AND RESIDUALS FOR ST21 (NO FAILURE CONDITION)

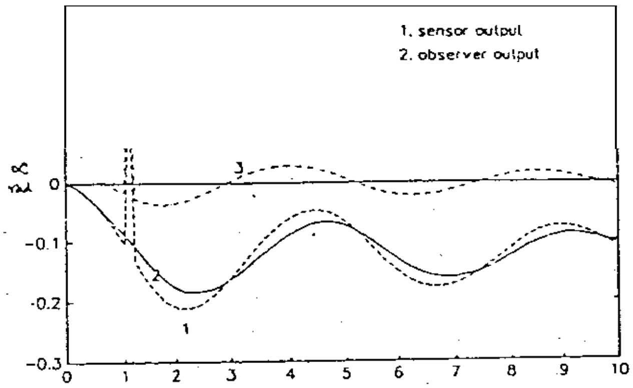


Fig 7. OBSERVER AND SENSOR OUTPUTS AND RESIDUALS FOR ST11 (FAILURE CONDITION: RECONFIGURED AFTER FAILURE DETECTIO