Fault-tolerant control of the ship propulsion system benchmark

Claudio Bonivento, Andrea Paoli*, Lorenzo Marconi
Department of Electronic, Computer Science and Systems, University of Bologna, Via Risorgimento 2, 40136 Bologna, Italy
Received 18 May 2001; accepted 11 March 2002

Abstract

The application of a new fault-tolerant control methodology to the benchmark proposed in Zamanabadi and Blanke (Control Engineering Practice 7(2) (1999)) is considered. The benchmark regards the model of a propulsion system for a marine vehicle developed by the Control Engineering Department of Aalborg University. After a brief description of the system, a fault analysis is carried out leading to a set of possible faults and remedial actions. Then the fault detection and identification method, and the reconfigurationalgorithm are described. Simulations on the model illustrate the performance of the fault tolerant system for some selected fault scenarios. © 2002 Elsevier Science Ltd. All rights reserved.

Keywords: Fault tolerant control; Process control; Quantitative and qualitative methods of fault diagnosis; Marine systems; Observers

1. Introduction

Automated systems are vulnerable to faults such as defects in sensors or in actuators and failures in controllers or in control loop, which can cause undesired reactions and consequences as damage to technical parts of the plant, to personnel or to the environment. The main objective of the fault detection and isolation (FDI) research area, widely addressed from several points of view in the last years (see, besides others, Frank, 1990; Chen & Patton, 1999), is that to study methodologies for identifying and exactly characterizing possible incipient faults arising in predetermined parts of the plant. This is achieved for example designing a dynamical system (filter) which, processing input/output data, is able to detect the presence of an incipient fault and eventually to precisely isolate it (see, besides others, De Persis & Isidori, 2001).

This phase is then usually followed by the design of a fault tolerant control (FTC) namely by the design of a reconfiguration unit which, on the basis of the faults identified, performs control reconfiguration in order to achieve prescribed performances also for the faulty system.

Many strategies can be followed to carry out the reconfiguration of the plant. For example, mechanical reconfiguration such as switching between redundant hardware or mechanical parameters variation can be used to avoid faults effects. Moreover, on the basis of the information provided by the FDI filter or by an identification algorithm, an adaptive and reconfigurable control can be designed to compensate for the effect of the fault and fulfill performances constraint (see Chandler, Pachter, & Mears, 1995). This is the case of the so-called explicit fault tolerant control where the reconfiguration phase is carried out looking for a parameterized controller which is suitably updated by a supervisor according to the information provided by the FDI unit. Another approach to the problem (see Bonivento, Paoli, & Marconi, 2001), which can be defined as implicit, follows a different perspective to fault tolerance control. In particular, restricting the analysis to that faults whose side-effects in the system operation are suitably modelled, the aim is to design a controller which embeds an internal model of the fault and hence is able to intrinsically compensate for its effect, regardless its entity and without its explicit estimation. In other words, the control reconfiguration does not pass through an explicit FDI design but, indeed, is achieved by a proper design of a dynamic controller which is implicitly fault tolerant to all the possible faults whose model is embedded in the regulator. In this framework, the FDI phase which is
usually the starting point in the design of a FTC, is postponed to that of control reconfiguration since it can be carried out by testing the state of the internal model unit which automatically activates to offset the presence of the fault.

It is important to stress that in general the design of a reliable FDI/FTC unit has to tackle important problems which characterize real applications, such as the presence of unknown parameters affecting the model of the system, unknown dynamics neglected in the model, unknown disturbances acting the system, the lack of knowledge of a meaningful model of the fault effect, etc.: all these and other factors can affect the performances of the FDI and reconfiguration scheme in the sense that faults could be detected even if not really present (false alarms) or, in a more critical and dangerous scenario, faults can be not detected at all (or detected with unacceptable delay). Clearly, the design of FDI/FTC control unit with pre-specified performances can be better performed if the designer has real data concerning disturbances and uncertainties characterizing the plant. This, in general, allows to perform a design suitably tailored on the specific applications and carries to a more simple and more reliable FDI/FTC units.

This paper focuses on the design of a FDI/FTC control unit for the benchmark of the ship propulsion system proposed in Blanke, Zamanabadi, and Bøgh (1997). This benchmark has been developed by the Control Engineering Department of Aalborg University (all the MATLAB/SIMULINK files as well as a complete description of the benchmark can be downloaded at the url http://www.control.auc.dk/ftc/) and it has drawn interest in control community since it faithfully reproduces the real behavior of the ship in terms of disturbances acting on the system, of behavior of internal dynamics, of non-linearities present in the plant. It is shown how to design a simple and reliable unit able to detect and isolate any possible faults proposed in the benchmark, and how to perform control reconfiguration able to preserve tracking performances for the controlled variables.

The paper is organized as follows. After a brief description of the overall benchmark, given in more detail in Zamanabadi and Blanke (1999), the paper presents the analysis of the possible faults acting on the system on the basis of the so-called failure mode and effects analysis (FMEA), see Zaitri, Keller, Barody, and Fleming (1991), Zamanabadi (1999), which represents an internationally accepted method for the classification of the faults (and hence for the evaluation of their gravity).

Then a simple FDI strategy is described, which allows perfect isolation of the three possible faults proposed in the benchmark. The information provided by the FDI unit are then used to develop a control reconfiguration structure in order to achieve a fault tolerant control system, able to preserve pre-specified performance also for the faulty system. Simulation results, showing the effectiveness of the control structure presented in the paper, conclude the work.

2. Ship propulsion system

The system described in this chapter is a propulsion system with one engine and one propeller for a marine vehicle as described in Zamanabadi and Blanke (1998). The scheme of the propulsion system is drawn in Fig. 1. This system is composed by the propeller pitch control system, the governor, which controls the fuel index of the diesel engine, the diesel engine, which generates a torque applied to the shaft, the propeller and the ship speed dynamics. Above those components, a coordinated controller calculates set-points for shaft speed $n_{\text{ref}}$ and for propeller pitch $\theta_{\text{ref}}$. For more details about the way $n_{\text{ref}}$ and $\theta_{\text{ref}}$ are generated the reader is referred to Zamanabadi and Blanke (1999).

The objective of the propulsion system is to maintain the ship’s ability to propel itself and to maneuver,
varying shaft speed and propeller pitch in a coordinated manner. Control is achieved by a two levels scheme: a higher level gives optimal set points for shaft speed and propeller pitch, while a lower level, made by two basics control loops, makes the propeller pitch and the shaft speed to track the references. A more detailed description of each subsystem is given in the following.

2.1. Propeller pitch control

The propeller pitch system, which is shown in Fig. 2, is approximated by a simple integrator which models the pitch dynamics and a proportional controller. Defining \((\theta_{\text{max}}, \theta_{\text{min}})\) the rate limits set for the hydraulic actuator, the overall system is described by

\[
\dot{\theta} = \max\{\dot{\theta}_{\text{min}}, \min(u_{\theta}, \dot{\theta}_{\text{max}})\},
\]

where \(\theta_{\text{m}}\) is the measured propeller pitch, perturbed by a noisy signal \(v_{\theta}\), and

\[
u_{\theta} = K_{\theta}(\theta_{\text{ref}} - \theta_{\text{m}}).
\]

2.2. Governor

The structure of the governor, generating the fuel index \(Y\) which represents the input of the diesel engine, is sketched in Fig. 3. The variable \(Y\) is generated by a classical PI controller acting on the error between the reference and the measured shaft speeds, \(n_{\text{ref}}\) and \(n_{\text{m}}\), respectively. The output of the PI controller, which also includes an anti-windup circuit, is then processed to assure that nonnegative or abnormal large values for the fuel index are generated. Further details about the structure of the PI controller and the algorithm to guarantee feasible values of \(Y\) can be found in Zamanabadi and Blanke (1999).

2.3. Diesel engine and shaft dynamics

The diesel engine, generating a torque \(Q_{\text{eng}}\) needed to turn the shaft, is modeled by a first-order dynamic described in the Laplace domain by

\[
\frac{Q_{\text{eng}}(s)}{Y(s)} = \frac{k_{y}}{1 + \tau_{c}s}.
\]

The shaft dynamics is described by a first-order differential equation

\[
I_{\text{m}}\dot{n} = Q_{\text{eng}} - Q_{\text{prop}},
\]

where \(Q_{\text{prop}}\) is the load torque generated by the propeller described in the following subsection.

2.4. Propeller characteristics

The thrust \(T_{\text{prop}}\) moving the ship, and the load torque \(Q_{\text{prop}}\) which acts against the \(Q_{\text{eng}}\), obeys to complicated formulas and depends on the shaft speed \(n\), the propeller pitch \(\theta\) and the speed of the ship \(U\). In this model, \(T_{\text{prop}}\) and \(Q_{\text{prop}}\) are calculated by interpolating real data measured under sea operation as described in Zamanabadi and Blanke (1999).

2.5. Ship speed dynamics

Denoting by \(M\) the mass of the ship, the dynamic of the speed \(U\) is governed by the following equation

\[
M\dot{U} = R(U) + (1 - t)T_{\text{prop}} - F_{\text{ext}},
\]

where \(F_{\text{ext}}\) is the external force acting on the ship.
where $T_{ext}$ represents the external force acting on the ship due to wind and waves, $r$ is a constant coefficient taking values in [0.05, 0.2] modeling the loss of a part of the propeller thrust due to the water flow in the area behind the ship, while $R(U)$ is the hull resistance dependent on the ship speed and its loading condition.

### 3. Fault scenarios

In this section, the faults which have been taken into account and the adopted failure modes and effect analysis (FMEA) methodology (see Zaitri et al., 1991; Blanke, Borch, Allasia, & Bagnoli, 1999; Toola, 1993) to classify their severity are given, as suggested in Zamanabadi (1999). The FMEA procedure is a powerful and standardized method to present a formalized manner the causes and the effects of the faults in a hierarchical model of a system. According to the description of the benchmark in Zamanabadi and Blanke (1999), three kind of faults have been considered:

1. A first class of faults are related to propeller pitch measurement. The propeller pitch is measured by a potentiometer which, due to broken wire or short circuit, yields a measure shifted by a constant value $\Delta \theta$, i.e.

   \[ \theta_m = \theta + v_0 + \Delta \theta. \]

   The offset $\Delta \theta$ can be positive or negative and its sign influences the severity of the fault as shown in Table 1. An increase of signal $\theta_m$, means a decrease of control action $u_p$. Since $\theta$ can be negative, this kind of fault can lead to a decrease of ship speed and also to a change of direction of the ship. On the other side if $\Delta \theta$ is negative, this leads to an increase of ship speed which means a very high risk of collision.

2. The second class of faults regards the shaft speed measurement which is performed by a tachometer. Analogously to the previous class, also this class of faults exhibits as a constant offset $\Delta n$ on the speed measurement, namely

   \[ n_m = n + v_n + \Delta n. \]

   The sign of the offset is determined by the kind of electro magnetic interference (EMI) disturbance generating the fault. In particular, it turns out that $\Delta n$ is positive if the EMI disturbance presents just on one pick-up of the tachometer, while it is negative if both the pick-up are involved. If $\Delta n$ is positive the fuel index decreases leading to a decrease of ship speed but, due to the architecture of the system, it is impossible that the ship change direction, being this effect due just to the pitch angle. However, if $\Delta n$ is negative, this leads to an increase of $Y$ and consequently to an increase of ship speed.

3. The last class of faults is related to the diesel engine. In particular, the fault which can be encountered is given by a loss of gain $\Delta K_y$ in the gain constant $K_y$ of the engine, namely

   \[ K'_y = K_y \Delta K_y \]

   with $\Delta K_y \in [0.1, 1]$. Since $K_y$ is < 1 this kind of fault can lead just to a decrease of $n$, i.e. a decrease of ship speed. This means that its severity level is not so high.

### 4. Fault detection and isolation methodology

The basic assumption used in developing the FDI scheme, is that the faults can occur independently and just when the reference signals $n_{ref}$ and $\theta_{ref}$ are constants and the system has reached the steady state. Under this assumption, bearing in mind the diagram sketched in Fig. 1, it is easy to realize that variations of the state value of the governor (whose structure is shown in Fig. 3) can be due to possible faults ($\Delta \theta$, $\Delta n$, $\Delta K_y$) affecting the sensors and the actuators and external noises ($T_{ext}$, $v_n$, $v_g$). Simple numerical analysis can be used to show that, assuming typical values for the faults and for the noises, it is possible to separate the effect which the faults and the noises have on the governor state. To this regard, we have simulated a particular faults sequences, using realistic values for faults and noises (see Table 2) as reported in the benchmark description Zamanabadi and Blanke (1999), and obtained the behavior of the variable $\Delta Y$ shown in the upper plot of Fig. 4. From this it is evident that a simple threshold (taken equal to $T_1 = 0.005$) can be used to

### Table 1

<table>
<thead>
<tr>
<th>Fault</th>
<th>End effect</th>
<th>Consequences</th>
<th>Severity level</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Delta \theta &gt; 0$</td>
<td>Decreased or reversed ship speed</td>
<td>Maneuvering risk, cost increase</td>
<td>High</td>
</tr>
<tr>
<td>$\Delta \theta &lt; 0$</td>
<td>Increased ship speed</td>
<td>Collision risk</td>
<td>Very high</td>
</tr>
<tr>
<td>$\Delta n &gt; 0$</td>
<td>Decreased speed ship</td>
<td>Maneuvering risk, cost increase</td>
<td>High</td>
</tr>
<tr>
<td>$\Delta n &lt; 0$</td>
<td>Acceleration</td>
<td>Collision risk</td>
<td>Very high</td>
</tr>
<tr>
<td>$\Delta K_y$</td>
<td>Decreased ship speed</td>
<td>Cost increase, diesel overload</td>
<td>Medium</td>
</tr>
</tbody>
</table>
generate a “pre-alarm” signal $Al_1$, namely

$$Al_1 = \begin{cases} 
0 & \text{if } -T_1 \leq \Delta Y \leq T_1, \\
1 & \text{otherwise.} 
\end{cases} \quad (3)$$

The goal of $Al_1$ is just to indicate to the high level control that a fault has been detected (detection phase).

The complete isolation of the faults can be achieved by generating more alarm signals as described in the following. In particular, the next two subsections present possible strategies to generate signals able to isolate the faults $\Delta \theta$ and $\Delta K_y$. These signals, joined to the pre-alarm signal $Al_1$, allow a complete isolation of the three faults.

### 4.1. Isolation of a loss of gain in diesel engine

The goal of this part is the design of dynamic block in order to generate an alarm signal influenced by the faults $\Delta K_y$ and $\Delta \theta$ but insensitive to $\Delta n$. To this end a fictitious observer of the ship speed (whose value is indeed exactly read) is designed and the error between the estimated and the real speed is used as further alarm signal. The computations which follow are devoted to find a simple observer of $U$ whose dynamics are influenced by the faults $\Delta K_y$ and $\Delta \theta$.

Bearing in mind (1) and (2), simple computations show that the dynamics of $U$ and $n$ are governed by the equations

$$m\ddot{U} = R(U) + (1 - t)T_{prop}(n, \theta, U) - T_{ext},$$

$$\dot{n} = -\frac{\dot{n}}{\tau_c} - \frac{\dot{Q}_{prop}(n, \theta, U)}{I_m} - \frac{\dot{Q}_{prop}(n, \theta, U)}{\tau_c I_m} + \frac{k_y Y}{\tau_c I_m}. \quad (4)$$

In view of this a simple observer of the ship speed is given by

$$m\ddot{\hat{U}} = R(U_m) + (1 - t)T_{prop}(\hat{n}^*, \theta_m, U_m) + F(U_m - \hat{U}),$$

$$\dot{\hat{n}}^* = -\frac{\dot{n}^*}{\tau_c} - \frac{\dot{Q}_{prop}(\hat{n}^*, \theta_m, U_m)}{I_m} - \frac{\dot{Q}_{prop}(\hat{n}^*, \theta_m, U_m)}{\tau_c I_m} + \frac{k_y Y}{\tau_c I_m}. \quad (5)$$

where $F$ is the constant observer gain, $\hat{U}$ is the estimated speed and $\hat{n}^*$ is an extra variable introduced in order to obtain a dynamic which is affected also by the diesel engine gain $k_y$.

Defining the estimate error as

$$\tilde{U} = U_m - \hat{U} \quad (6)$$

the error dynamic is given by

$$m\ddot{\tilde{U}} = (1 - t)T_{prop}(n, \theta, U_m) - T_{ext} - (1 - t)T_{prop}(\hat{n}^*, \theta_m, U_m) - F \hat{U}. \quad (7)$$

<table>
<thead>
<tr>
<th>Fault</th>
<th>Magnitude</th>
<th>Start (s)</th>
<th>End (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Delta \theta$</td>
<td>1 rad</td>
<td>180</td>
<td>210</td>
</tr>
<tr>
<td>$\Delta n$</td>
<td>13 rad/s</td>
<td>680</td>
<td>710</td>
</tr>
<tr>
<td>$\Delta \theta$</td>
<td>-0.7 rad/s</td>
<td>1909</td>
<td>1920</td>
</tr>
<tr>
<td>$\Delta n$</td>
<td>-1 rad/s</td>
<td>2640</td>
<td>2670</td>
</tr>
<tr>
<td>$\Delta K_y$</td>
<td>0.2</td>
<td>3000</td>
<td>3500</td>
</tr>
</tbody>
</table>

Table 2
Fault sequence adopted for numerical analysis as described in Zamanabadi and Blanke (1998)

Fig. 4. Numerical analysis using the fault sequence described in Table 2. From the upper to the lower plot are shown the behaviors of $\Delta Y$, $\Delta \theta$, and $\hat{U}$. 

---

or, collecting the terms influenced by the thrust,

\[ m\dot{U} = -T_{\text{ext}} + \Delta T_{\text{prop}}(\Delta k, \Delta \theta, v_0) - F\dot{U}, \]

where \( \Delta T_{\text{prop}} \) is a suitably defined nonlinear function which depends on the faults \( \Delta \theta \), \( \Delta k \) and on the sensor noise \( v_0 \). The terms \( T_{\text{ext}} \) and \( \Delta T_{\text{prop}} \) in (8) represent drift terms due to unmeasurable variable. Both these terms are saturated, so the estimation error \( \dot{U} \) will not converge to zero, but will converge to a finite value dependent on \( T_{\text{ext}} \) and \( v_0 \) in faulty case also on \( \Delta k \) and \( \Delta \theta \). For this reason, in order to qualify the variable \( \dot{U} \) as alarm signal, it is needed to check the sensitivity of this variable to the faults \( \Delta \theta \), \( \Delta k \), and evaluate the influence of the noise \( T_{\text{ext}} \) and \( v_0 \). To this end, we simulated the behavior of \( \dot{U} \) assuming again the faults scenario reported in Table 2 and we obtained the result shown in the lower plot in Fig. 4. In light of this numerical inspection, the alarm signal \( Al_2 \) can be generated by comparing the value of \( \dot{U} \) with a threshold (which has been fixed to \( T_2 = 0.006 \)), namely

\[ Al_2 = \begin{cases} 0 & \text{if } -T_2 \leq \dot{U} \leq T_2, \\ 1 & \text{otherwise}. \end{cases} \]

### 4.2. Isolation of a sensor failure

A simple reliable strategy to detect a sensor fault, is to check the propeller pitch control variable which is generated by the proportional controller \( K \) (see Fig. 2). In nominal steady state conditions, i.e. in absence of the fault \( \Delta \theta \) and sensor noise \( v_\theta \), the control action is clearly zero. Hence, a possible deviation from the zero value can be due both to the fault or noise. Since the maximum deviation of the noise (see Zamanabadi & Blanke (1999)) is 0.0425 rad and the gain of the pitch controller is \( k_1 = 0.15 \), it is easily realized that a simple threshold equal to \( T_1 = 0.0065 \) allows the fault isolation. In other words an alarm signal \( Al_3 \) can be generated as

\[ Al_3 = \begin{cases} 0 & \text{if } -T_3 \leq \dot{\theta}_m - \dot{\theta}_{\text{ref}} \leq T_3, \\ 1 & \text{otherwise}, \end{cases} \]

(10)

to selectively detect the fault \( \Delta \theta \). For completeness the behavior of \( u_\theta = K_1(\dot{\theta}_m - \dot{\theta}_{\text{ref}}) \) in presence of the faulty conditions reported in Table 2 is shown in the middle plot of Fig. 4. As expected \( u_\theta \) is sensitive just to the fault on the potentiometer which, in turn, is distinguishable from the noise affecting the measure.

### 5. Reconfiguration strategy

Once a fault has been detected and isolated, the next step is to reconfigure the system in order to guarantee prescribed performances also for the faulty system. The

<table>
<thead>
<tr>
<th>Actions in case of combinations of signals Al1, Al2 and Al3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Al1</td>
</tr>
<tr>
<td>Al2</td>
</tr>
<tr>
<td>Al3</td>
</tr>
<tr>
<td>Al1 and [not(Al2)] and [not(Al3)]</td>
</tr>
<tr>
<td>Al1 and Al2 and [not(Al1)]</td>
</tr>
<tr>
<td>Al1 and Al2 and Al3</td>
</tr>
<tr>
<td>Al1, Al2 and Al3</td>
</tr>
</tbody>
</table>

Reconfiguration actions are summarized in Table 3. Different strategies have been adopted in case of a fault on the diesel engine or a fault on a sensor.

#### 5.1. Loss of gain in the diesel engine

The reconfiguration strategy needed to offset the loss of gain in the diesel engine is basically guaranteed by the integrator embedded in the governor dynamic. As a matter of fact it is trivial to see that, as far as the loss of gain does not affect the stability of the loop, the integral action is able to automatically provide the extra control effort needed to compensate for \( \Delta n \). In other words, the system is implicitly fault tolerant to this kind of failure. So a loss of gain in the diesel engine leads to a transient, characterized by a lower ship speed, but, after this period, the control error returns to zero. For this reason, and considering that this failure is a medium risk one, no other actions are taken.

#### 5.2. Additive faults on sensors

Considering the other two kinds of failure, it is easy to see that an additive error on a sensor measure leads to a definitive loss of reference and a reconfiguration of control system is unavoidable. The strategy used to compensate the sensors faults consist of reconfiguring the reference signals. In other words, a “dummy” reference signal is designed in real time in order to offset the additive signal on the feedback loop, namely

\[ \dot{n}_{\text{ref}} = n_{\text{ref}} \pm \Delta n, \]

\[ \dot{\theta}_{\text{ref}} = \theta_{\text{ref}} \pm \Delta \theta, \]

(11)

where \( \Delta n \) and \( \Delta \theta \) are estimate of the faults on shaft speed and pitch angle sensors, respectively. In particular, \( \Delta n \) and \( \Delta \theta \) are identically zero in case the alarm signals are zero and computed according to simple inversion algorithms in case a fault has been detected. In detail, as the fault on the pitch angle sensor is concerned, we adopted the following updating law.
for the estimation $\Delta \hat{\theta}$

$$\Delta \hat{\theta} = \theta_{\text{ref}} - \left[ \frac{1}{s} + \frac{1}{K_{\text{e}}} \right] u_{\text{q}},$$

(12)

where $u_{\text{q}}$ is the action provided by the analog actuator of the pitch angle, supposed to be measurable.

In short, the control reconfiguration of the pitch angle dynamics consists, once a fault $\Delta \theta$ has been detected at time $t^\star$ (namely when $A_1$ jumps to one), of running the dynamics (12) from the initial condition $\Delta \hat{\theta}(t^\star) = 0$ and updating the reference signal $\theta_{\text{ref}}$ according to (11). Of course, the effectiveness of this reconfiguration strategy is affected by the reliability of the estimation $\Delta \hat{\theta}$. The latter is influenced on one hand from the initial condition $\Delta \hat{\theta}(t^\star)$ (which in principle should be set to zero at the same time in which the fault happens but that, in practice, is initialized just when the fault is detected) and, on the other, from the presence of the unknown disturbance $v_g$. As far as the initialization is concerned it is worth just noting that the instance in which $A_1$ raises corresponds to that in which the fault occurs (see the mechanism with which $A_1$ is generated in (10)) and hence this does not affect considerably the estimation. On the contrary, trivial computations shows that the disturbance $v_g$ introduces an estimation error equal to

$$\Delta \hat{\theta}(t) - \Delta \hat{\theta}(t^\star) = v_g(t^\star) - v_g(t).$$

Hence, in view of the fact that $|v_g| \leq 0.0425$, it turns out that the maximum estimation error is always lower than 0.085.

As the shaft speed sensor fault is concerned, we used the following reconfiguration strategy. Once the alarm signal $A_1$ goes to one (namely when a not well defined fault occurs), the updating law

$$\Delta \hat{n} = n_m - \hat{n},$$

$$\hat{n} = \frac{1}{s \lambda_m} (Q_{\text{eng}} - Q_{\text{prop}}(\theta_m, \hat{n}, U_m))$$

(13)

is run from the initial condition $\Delta \hat{n}(t^\star) = 0$ and the reference signal $n_{\text{ref}}(t)$ modified according to (11) just if, besides $A_1 = 1$, both $A_2$ and $A_3$ remain to zero after a prescribed settling time $T_w$. Clearly in Eq. (13)

$$Q_{\text{eng}} = \frac{k_2}{1 + \eta_\lambda s} Y,$$

$$n_m = n_{\text{ref}} - e_Y$$

and $e_Y$ is computed via the measurements of $Y$ by

$$e_Y = \frac{s}{k_\lambda s + k_1} Y.$$

Clearly, the motivation to run dynamic (13) when $A_1$ raises is to reduce the estimation error induced by a wrong initial state (to this end note that a possible jump of $\Delta n$ induces a jump of $A_1$, see (3)). On the other hand, the reason for waiting the settling time $T_w$ to eventually modify the reference signal $n_{\text{ref}}$ is clearly motivated to guarantee that the fault occurred is really $\Delta n$.

Similarly to the estimation of the pitch angle fault, also the error $\Delta \hat{n}(t) - \Delta n(t)$, and thus the effectiveness of the reconfiguration strategy, is affected by the measure disturbance $v_n$. Simple computation allows to find that

$$\Delta n(t) - \Delta \hat{n}(t) = v_n(t^\star) - v_n(t)$$

and hence, in view of the fact that $|v_n| \leq 0.0625$, we conclude that the maximum estimation error is always lower than 0.125.

6. Simulation results

In order to check the effectiveness of the procedure above proposed, a certain number of tests have been made, simulating few faulty or healthy conditions. In all these tests the value chosen for the observer gain is $F = 100$.

In a first time just single faults have been simulated using the reference signals given in the benchmark. More in details a fault on shaft speed sensor of $\Delta n = 7.5675 \text{ rad/s}$ occurred after 2403 s from the beginning has been simulated leading to the results shown in Fig. 5.

Then a fault on propeller pitch angle sensor described by $\Delta \theta = -0.86 \text{ rad}$ occurred after 1349 s has been taken in account and the obtained results are sketched in Fig. 6.

To conclude this first simulation part, a loss of gain on diesel engine has been simulated. More in detail we assumed that after 1000 s $\Delta k_\lambda = 10\%$. The results of this simulation have been plotted in Fig. 7.

In all these plots the ship speed is shown both in case of reconfiguration and in case when no control modifications are taken (with the exception of the case of a loss of gain of the diesel engine in which, as described above, no explicit reconfiguration is adopted). It is possible to see that, for all the possible faults, the control reconfiguration assures tracking of the reference signal (super-imposed in the plots).

To test the control strategy presented in the paper in a more general situation, we generated different (from that proposed in the benchmark) references, assuming random (more than one) faults and random references (generated within the constraints given in Zamanabadi & Blanke (1999)). In Table 4 some meaningful results are reported with in particular the time elapsed from the fault and its isolation time.

In these tests we obtained 0% of false alarm, 0% of missed diagnosis and 0% of bad isolation with a delay of about 8 s in $\Delta n$ isolation, 2 s in $\Delta \theta$ isolation and about 4 s as $\Delta k_\lambda$ failure is concerned. In this respect, the differences between the isolation times for the faults, is clearly due to the necessity of synchronizing the
Diagnosis signals. In fact, in case of $\Delta \theta$, since there is just one signal involved in diagnosis ($A_{13}$) the isolation time is lower than in other faulty cases ($\Delta \omega$ and $\Delta k_y$) where more than one signal is involved in the fault isolation procedure. By the way it is important to stress that the time to detect for each fault, both single and multiple ones, is always lower than 10 samples so that, as the sample time is 1 s (see Zamanabadi & Blanke, 1999), the time-to-detect requirements given in Zamanabadi and Blanke (1999) are satisfied.

7. Conclusions

In this article, a simple design of a fault tolerant control system applied to a ship propulsion system has
After a brief description of the system a fault and risk analysis has been carried out and a set of possible remedial actions has been found. Then the synthesis of the control system, concerning the design of fault diagnosis algorithm and system reconfiguration algorithm, has been described. It is important to note that in the first part of the article, as suggested by the benchmark description (see Zamanabadi & Blanke, 1999), we considered sensors faults limited to offset faults, but, since neither the FDI methods nor the reconfiguration strategy are dependent on the behavior of faults, it is possible to relax this constraint. The only requirement for successful FDI and reconfiguration is that the faults on sensors occur abruptly. This let us to consider also more realistic sensors faulty conditions, like physical or electrical damages, which can make the sensors to generate a zero output or a maximum output. Simulations results obtained in a general scenario of faults have shown the effectiveness of the control strategy used.

References


Table 4
Simulation results

<table>
<thead>
<tr>
<th>Experiment no.</th>
<th>Fault</th>
<th>Time (s)</th>
<th>Magnitude</th>
<th>Isolation time (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$\Delta k_y$</td>
<td>895</td>
<td>15%</td>
<td>899</td>
</tr>
<tr>
<td>2</td>
<td>$\Delta \theta$</td>
<td>1250</td>
<td>0.5 rad</td>
<td>1252</td>
</tr>
<tr>
<td>3</td>
<td>$\Delta \eta$</td>
<td>2500</td>
<td>-4.56 rad/s</td>
<td>2508</td>
</tr>
<tr>
<td>4</td>
<td>$\Delta k_y$</td>
<td>1000</td>
<td>15%</td>
<td>1003</td>
</tr>
<tr>
<td>5</td>
<td>$\Delta \eta$</td>
<td>3100</td>
<td>6.76 rad/s</td>
<td>3109</td>
</tr>
<tr>
<td>6</td>
<td>$\Delta \theta$</td>
<td>3010</td>
<td>0.8 rad</td>
<td>3012</td>
</tr>
<tr>
<td>7</td>
<td>$\Delta \eta$</td>
<td>400</td>
<td>10.1 rad/s</td>
<td>407</td>
</tr>
<tr>
<td></td>
<td>$\Delta \theta$</td>
<td>1080</td>
<td>-0.71 rad</td>
<td>1084</td>
</tr>
<tr>
<td></td>
<td>$\Delta k_y$</td>
<td>2232</td>
<td>11%</td>
<td>2236</td>
</tr>
</tbody>
</table>

Fig. 7. Simulation of a loss of gain on the diesel engine.
Claudio Bonivento was born in Bologna, Italy, in 1941. He graduated cum laude in Electrical Engineering from the University of Bologna in 1964. Since 1975, he has been Professor of Automatic Control in that University. He has held visiting positions at various academic institutions, which include the University of California at Berkeley, the University of Florida at Gainesville, the MIT in Boston. He served the Italian scientific community as President of GRIS (Italian Group of Researchers on Computer and Systems) in the period 1981–82, and as President of CIRA (Italian Inter-university Centre of Research on Automatica), during the period 1989–1992. In 1986, he promoted the constitution of LAR (Laboratory of Automation and Robotics) at the Department of Electronics Computer and Systems, University of Bologna. In 1990 he launched the centre for multimedia technologies for education of the same University. From 1993 to 1996 he was the co-ordinator of ERNET (European Robotics research Network) in the framework of the Human Capital and Mobility programme of the European Union. Since 1994, he has been a member of the Italian delegation at the IFAC. His main research interests are in control systems theory, fault detection and diagnosis, and robotic manipulation. He is author or co-author of about 160 technical and scientific publications. He is author or co-author of five books on applied mathematics, digital control systems, and system identification and simulation. Professor Bonivento is also active in industrial control applications, at present with specific interest in automatic machinery for packaging and automotive areas. Professor Bonivento is a senior member of IEEE, and an elected member of the Administrative Council of EUCA (European Union Control Association) for the 2-term 1997-2002. Since November 2000, he is Director of DEIS (Department of Electronics Computer Science and Systems), University of Bologna.

Lorenzo Marconi was born in Rimini, Italy, in 1970. He graduated in 1995 at University of Bologna. Since 1995 he has been with the Department of Electronics, Computer Science and Systems at University of Bologna, where obtained his Ph.D. degree in March 1998. Since 1999 he is Researcher in Automatic Control at the same Department. From August to December 1997 and from November to December 1998 he held visiting positions at the Department of Systems Science and Mathematics, Washington University, St. Louis. His current research interests include nonlinear control, output regulation, geometric approach, fault detection.

Andrea Paoli was born in Fano, Italy in 1975. He received the Laurea degree in computer science engineering from the University of Bologna in 2000. He is currently a PhD student at the Dipartimento di Informatica e Sistemistica at the University of Bologna, Italy. His current research interests focus on Fault Tolerant Control systems and Fault Diagnosis in distributed systems.