Fault-tolerant control of continuous-variable system: Reconfiguration strategy for the three tanks system

John Florescu, Australian College of Kuwait, P.O.Box 1411 Safat, 13015 Kuwait

***Abstract* — Fault-tolerant or reconfigurable control systems are generally based on a nominal control law related to fault detection and isolation. This paper describes a fault-tolerant control (FTC) system design technique for a non linear system detectable by observation. The redundant hardware is used to compensate for faults. The method outlined in this paper relies on the system behavior of all the components involved. During the reconfiguration process, the forward controls are maintained and the modifications are performed only in the feedback. The switching function also serves as the fault indicator. It is demonstrated that the transient periods are minimal and the performance of the reconfigured system remains the same**

***Index Terms* — Fault tolerance, Modeling, reconfigurable architectures, observers.**

I. Introduction

Many control systems are subject to faults in components such as sensors or actuators which can contribute to the malfunction of the system. The objective of fault tolerant control systems is to disallow one or several faults to develop into overall system failure. The process of fault diagnosis has three steps: *detection, isolation, reconfiguration or accommodation.*
Numerous systems have been proposed to test design fault tolerant control (FTC) systems. The three-tank bench problem captures the continuous dynamics of the system and demonstrates a way to compensate for the faults.

Detection of faults and isolation ensures that the systems do not lead to a reduction in performance or a breakdown. This paper suggests a solution that generates suitable inputs for the faulty plant based on the output of the nominal controller.

It is proven that an automatic reconfiguration in the case of actuator faults implies a larger number of control inputs than the number of controlled outputs according to Boskovic, J. D., et. al. (1998), "A stable scheme for automatic control reconfiguration in the presence of actuator faults" [1].

Many fault tolerant controller strategies implemented and described in references A. Fekih, F.N Chowdhury, "A robust fault tolerant control strategy for a class of nonlinear uncertain systems"[2] and H. Niemann, "Fault tolerant control based on active fault diagnosis" [3] exist using a classical observer to compare the real system with the model. The redundant components in the system must be used to ensure the same response from the reconfigured control system.

II. Problem Statement

The three-tank system consists of three water tanks connected by pipes. The connected pipes are fitted with valves. The system has two pumps: one belonging to the nominal system and a redundant one as shown in **FIGURE 2.**.

The parameters and the variables are described in M. Blanke, M. Kinnaert, J. Lunze, M. Staroswiecki, "Diagnosis and Fault-Tolerant Control", Springer ed [4].

Table A Parameters of the three-tank system

Parameter	**Value in SI unit**	**Description**
A	1.54×10^{-2} m^2	Cross-section area of tank
h_{max}	0.6 m	Height of the tank
h_H	0.6 m	Height of upper valve
c_{12L}	1.6×10^{-4} m^2/s	Flow constant valve V_{12L}
c_{12H}	1.6×10^{-4} m^2/s	Flow constant valve V_{12H}
c_{23L}	1.6×10^{-4} m$^{5/2}$/s	Flow constant valve V_{23L}
c_{23H}	1.6×10^{-4} m$^{5/2}$/s	Flow constant valve V_{23H}
c_2	1.6×10^{-4} m$^{5/2}$/s	Flow constant outlet of tank 2
c_L	1.6×10^{-4} m$^{5/2}$/s	Flow constant of leakage in tank 1
c_{P1}	1.0×10^{-4}m^3/s	Flow constant of pump 1
c_{P2}	1.0×10^{-4}m^3/s	Flow constant of pump 2
$q_{P1\max}$	2.0×10^{-4}m^3/s	Max. flow of pump 1
$q_{P2\max}$	2.0×10^{-4}m^3/s	Max. flow of pump 2
h_{1REF}	0.5 m	Set point for PI controller
h_{2L}	0.09 m	Position Lower sensor in Tank2
h_{2H}	0.11 m	Position Upper sensor in Tank2

k_P	6.0 l/m	Proportional gain for PI controller
k_I	15.0x10^{-2}l/ms	Integral gain of PI controller

Nominal case

The valves V_{12L}, V_{23H}, V_{23L} are closed.

For the nominal case only the left tank and the middle tank are in use. The right tank is used only in emergency.

The purpose of the tank system is to supply water to a consumer with a flow q_2.

Leakage in tank one is a possible fault.

The water level in the second tank is maintained between h_{2L} and h_{2H}.

In nominal conditions:

1. Only left and middle tanks are in used.
2. The level in the second tank is between h_{2L} and h_{2H}.
3. No leakage q_L=0.
4. The valves V_{12L}, V_{23L}, V_{23H} are closed. The water is supplied to the second tank via the top valve V_{12H}.
5. The level h_1 in the first tank is controlled continuously using pump P_1. The level in the first tank is maintained at reference level h_{ref}.
6. The valve V_{12H} is turned on and off by another controller to maintain the level in the second tank between h_{2L} and h_{2H}.

The water flow q_{ij} from Tank i to Tank j is calculated using *fluid mechanics laws*:

$$q_{ij} = c_{ij} sign\left(h_i - h_j\right)\sqrt{\left|h_i - h_j\right|} \quad (1)$$

The coefficients c_{ij}, depends on the geometry of the tanks and pipes.

The control system produces a set of signals to control the appropriate actuators in accordance with the information provided by sensors.

The control signals for the nominal controller are: u_1 for the pump P_1, u_2 for the valve V_{12H} and u_3 for the valve V_{12L}.

Reconfigurable case -a fault has been detected.

The reconfiguration control system may use additional control signals depending on the fault: u_4 for the pump P_2, u_5 for the valve V_{23H} and u_6 for the valve V_{23L}.

The assumption is that the sensors and the two controllers are working satisfactory. The two controllers are reused to control the redundant components in concordance with a predefined strategy.

Dynamic modeling of two water tank heights

The equation (1) is used in modeling the three tanks system.

$$\dot{h}_1 = \left(q_{P1} - q_{12L} - q_{12H} - q_L\right)/A \quad (2)$$

$$\dot{h}_2 = \left(q_{12L} + q_{12H} - q_{23L} - q_{23H} - q_2\right)/A \quad (3)$$

$$\dot{h}_3 = \left(q_{P2} + q_{23L} + q_{23H}\right)/A \quad (4)$$

The following substitutions are made in order to simplify the equations:

$z_{P1}=(q_{P1}\sqrt{h_1})/A$
$z_{12H}=(q_{12H}\sqrt{h_1})/A$,
$z_{12L}=(q_{12L}\sqrt{(h_1+h_H-h_2)})/A$,
$z_{P2}=(q_{P2}\sqrt{h_3})/A$,
$z_{23H}=(q_{23H}\sqrt{h_3})/A$,
$z_{23L}=(q_{23L}\sqrt{(h_3+h_H-h_2)})/A$,
$z_L=(q_L\sqrt{(h_1+h_H)})/A$,
$z_2=(q_2\sqrt{h_2})/A$

TABLE B shows the effect of control signals.

The +/- signs suggest the effect of the corresponding component on the system variable when operating.

For example, when valve V_{12H} is opened there is a negative impact on the level in Tank1, but a positive one on the level in Tank2.

There are three sensors in the system: one to measure continuously the level in Tank1 and two fix sensors in Tank2.

The three faults can be identified by reading of these three sensors.

Fault F1: valve V12H closed and blocked: $u_1<0$; $h_2<h_{2L}$

The control signal of the pump P1 was selected instead of the level in Tank1 to avoid triggering the detection of a fault during transition periods.

Fault F2: valve V12H opened and blocked: $h_2 < h_{2L}$

Fault F3: leakage in Tank1: $u_1 > 0.8$; $h_2 < h_{2L}$

When the pump is working more than 80%, a leakage is assumed.

A fault is indicated after the variable measurements show a large discrepancy which lasts for a relative long period.

A structural analysis of the system is described in M. Blanke, M. Kinnaert, J. Lunze, M. Staroswiecki, "Diagnosis and Fault- Tolerant Control" [5] and a similar one is shown below **FIGURE 2.**

The structural analysis provides useful information in the following areas:

- The identification of the components of the system .
- The existence of reconfiguration possibilities.
- The identification of the redundant components.

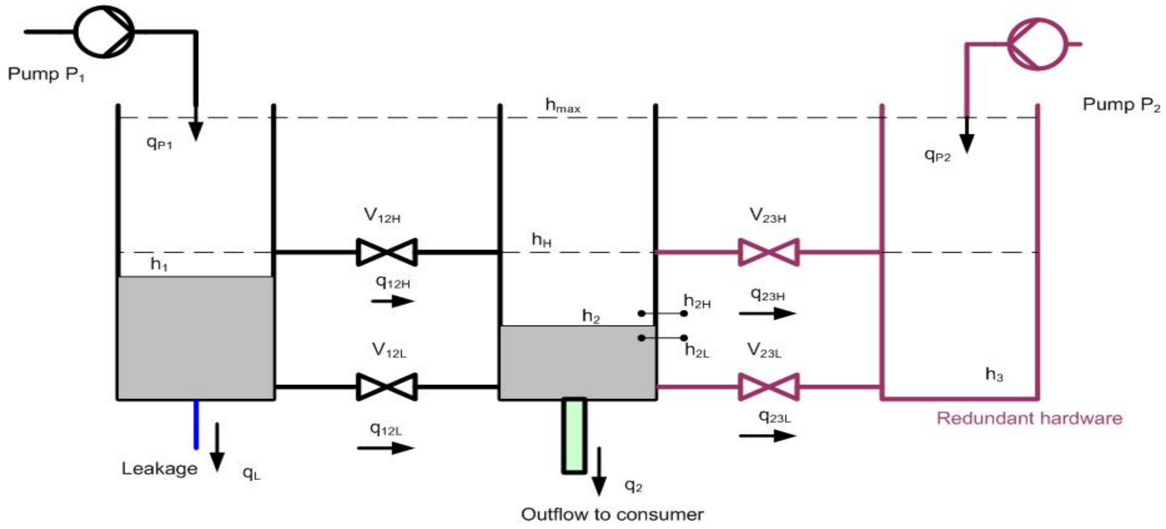

FIGURE 1 The tree tanks configuration

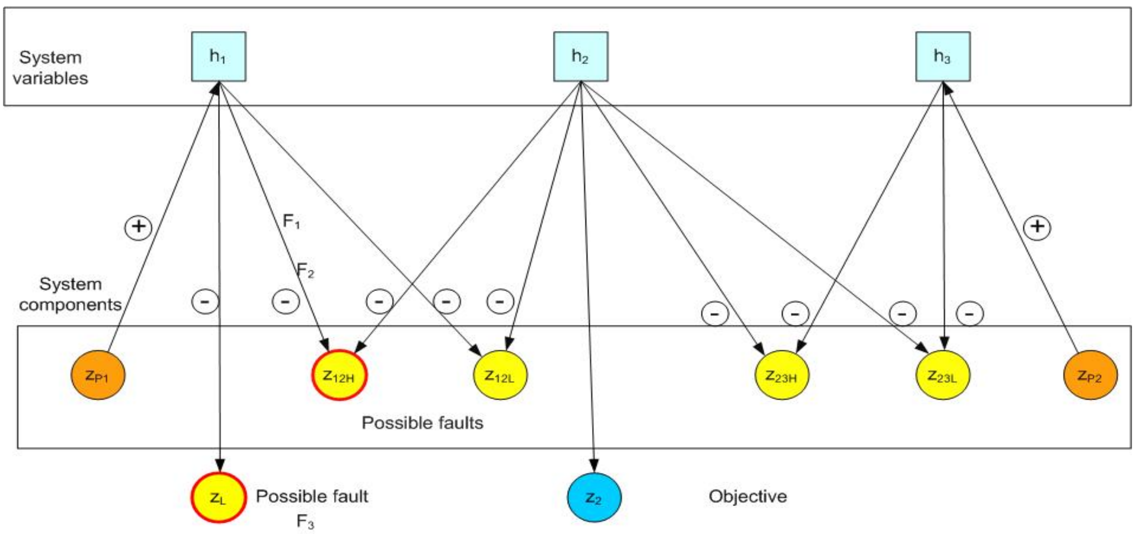

FIGURE 2 Graph - components contribution to system variables

Table B. The effect of control signals

Control signal	Component coefficient	Δh_1	Δh_2	Δh_3
u_1	z_{P1}	+	0	0
u_2	z_{12H}	-	+	0
u_3	z_{12L}	-	+	0
u_4	z_{P2}	0		+
u_5	z_{23H}	0	+	-
u_6	z_{23L}	0	+	-
leakage	z_L	-	0	0
outflow	z_2	0	-	0

The graph in FIGURE 2 shows the effect of the system components on the system variables. For example the pump 1 that is associated with the component coefficient z_{P1} has a positive effect on the level in tank1 (h_1). The valve V_{12H} represented by the coefficient z_{12H} and controlled by the signal u_2 has a negative effect on the level in Tank1 but a positive impact on level in Tank2. When V_{12H} is opened this allows the fluid from Tank1 to flow in Tank2.

III. RESULTS

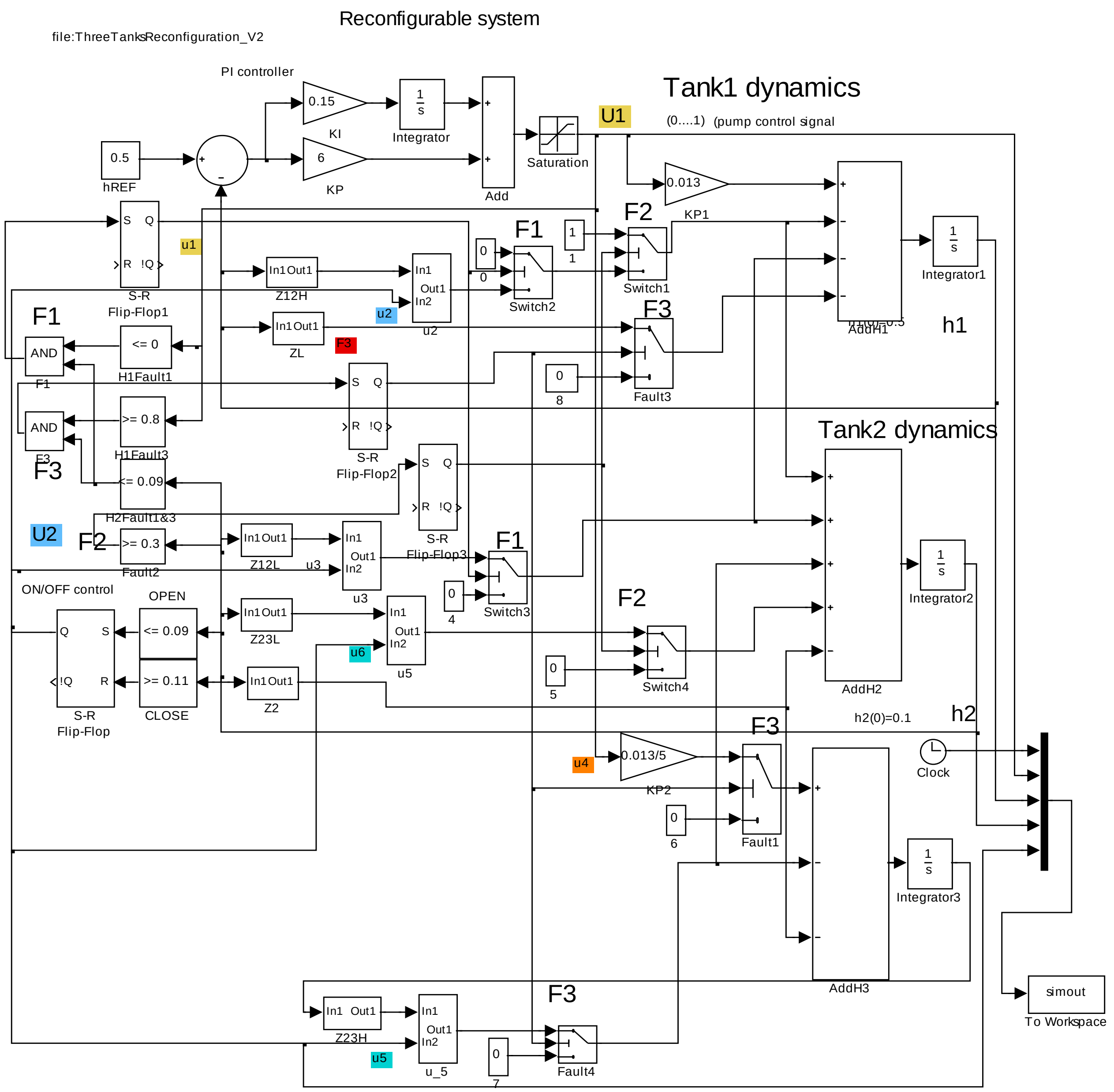

FIGURE 3. Simulink diagram of the proposed fault-tolerant control system

The faults F1, F2 and F3 are detected by an observer using Boolean functions and flip flops. Upon detection of a particular fault certain parameters of the controller are modified.
The main objective is to maintain a constant flow to the customer by keeping the level in Tank2 at a specified level. A secondary objective is to maintain the fluid level constant in Tank1. Even this objective is not essential the results show that this goal is achieved as well.

Figures 4a and 4b display the level in Tank1 and in Tank2 respectively when is no fault present.
The control signal for pump 1 is shown in FIGURE 4c.
The valve V_{12H} is either ON or OFF and the control signal to achieve this is shown in FIGURE 4d.
FIGURE 5 displays the variables and control signals when fault F1 is present (valve V_{12H} is blocked closed).
The system brings in the valve V_{12L} that has the control Signal u_3 as shown in TABLEB. FIGURE 5d shows how the ON/OFF controller operates the valve V_{12L}.

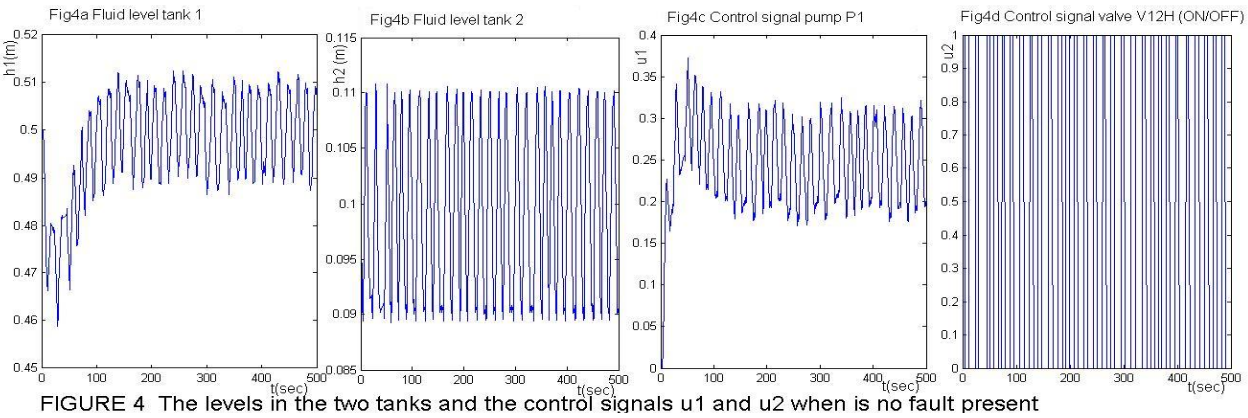

FIGURE 4 The levels in the two tanks and the control signals u1 and u2 when is no fault present

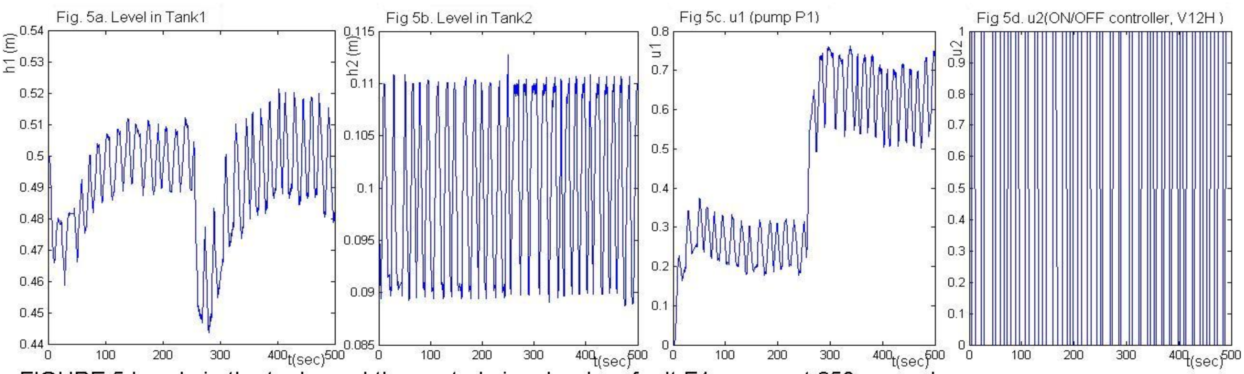

FIGURE 5 Levels in the tanks and the control signals when fault F1 occurs at 250 seconds

IV. Conclusions

When a fault occurs there may be a need to alter the control law to recover the system from the effects of failures. In this case the controllers play an active part in recovering from faults.

In this example the observer performs the fault detection as well as the system reconfiguration.

A pyramidal decomposition of the system is a very useful tool to identify and design a Fault Tolerant Controller. It readily assists evaluation of the amount of redundancy and its contribution in system recovery.

V. References

[1] Boskovic, J. D., et. al. (1998). “A stable scheme for automatic control reconfiguration in the presence of actuator faults,” *Proceedings of American Control conference, Philadelphia, Pennsylvania*, June, 1998, pp. 2455-2459.

[2] A. Fekih, F.N Chowdhury, “A robust fault tolerant control strategy for a class of nonlinear uncertain systems”, *Proceedings of the 2006 American Control conference Minneapolis, Minnesota*, USA, June 14-16, 2006.

[3] H. Niemann, “Fault tolerant control based on active fault diagnosis,” *2005 American Control Conference*, June 8-10, Portland, OR, USA.

[4] M.A. Sainz, J.Armengol, J.Veh, “Fault detection and isolation of the three-tanksystem using the Modal Interval Analysis”, *Departament d'Electrµonica, Informatica i Automatica*.
Universitat de Girona. Campus Montilivi. E-17071 Girona (Spain)

[5] M. Blanke, M. Kinnaert, J. Lunze, M. Staroswiecki, “Diagnosis and Fault- Tolerant Control”, Springer ed.

[6] J.L. Villa'J, M. Duque', A. Gauthier' and N. Rakoto-Ravalontsalama, **“**MLD Control of Hybrid Systems: Application to the Three-Tank Benchmark Problem”, *'Ecole des Mines de Nantes / IRCCyN 4***,** rue Alfred Kastler, F-44307 Nantes Cedex 03, France

[7] Tal Pasternak, “Reconfiguration in Hierarchical Control of Piecewise-Affine Systems”, *Institute for Software Integrated Systems*,
Department of Electrical Engineering and Computer Science Vanderbilt University.