Fault-Tolerant Control of Nuclear Steam Generator Water Level

Myung-Ki Kim

Korea Electric Power Research Institute,

Nuclear Power Laboratory,

103-18 Munji-dong, Yusong-gu, Taejon 305-380

Abstract

This paper is concerned with a fault-tolerant control with guaranteed H_∞ performance for nuclear steam generator. The fault-tolerant control having passive redundant structure guarantees both stability and faults of controllers and sensors. The systematic design method is drawn in terms of Linear Matrix Inequalities (LMIs). Also the sufficient condition of fault-tolerant control is provided. The computer simulation demonstrates the fault-tolerant control woks well under failure of controllers and in view of the performance it is superior to conventional PID controller.

I. Introduction

Traditionally there have been two approaches for dealing with increasing reliability of controlled systems. The first method is *active redundancy*, which relies on the process of fault detection, isolation, and reconfiguration to detect the presence of failures, to isolate them to a particular component, and then to reconfigure the system to restore acceptable operation [1], [2], and [3]. The second method, *passive redundancy*, accounts on the notion of fault masking, through clever design of the control law and the control configuration faults are naturally accommodated, loosely defined as minimizing the impact of faults on system performance, without recourse to external logic system. In work of [4], it gives a synthesis for a pair of controllers such that their sum stabilizes the plant and each of them also stabilizes the plant where the other one is fail. The design of fault-tolerant H_∞ control systems using observer-based output feedback were introduced in [5] and [6], provided that failure of sensor and actuator occur only within a prescribed subset of control components. [5] and [6] show a control synthesis for nominal systems and uncertain systems, respectively.

In this paper based on the passive redundant structure, we will try to develop the fault-tolerant control system with disturbance attenuation γ. Considering faults of controllers and sensors as system disturbances, The fault-tolerant control problem can be converted into the H_∞ norm bounding control

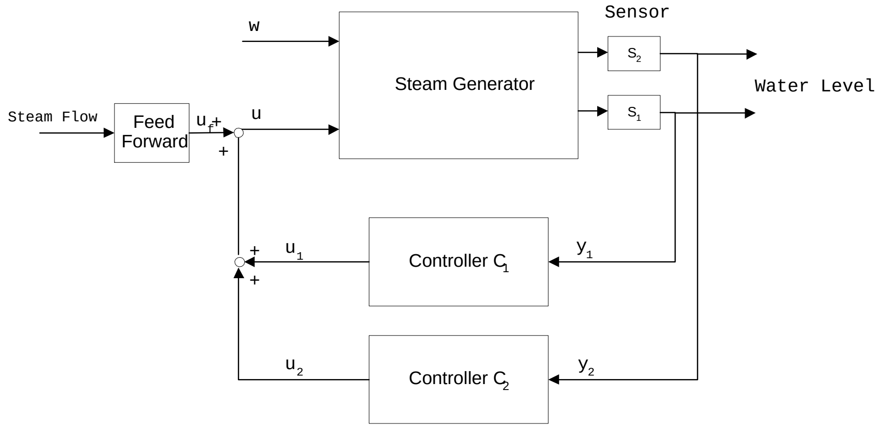

Fig. 1. Structure of faut-tolerant control.

problem, which is to determine the controller that stabilizes the closed-loop system, while bounding the H_∞ norm of the transfer function from the disturbance input to the regulated output by a given bound γ. Faults considered in this analysis includes not only hardware problems such as sticky actuators, controller faults and biased sensors, but also the system disturbance, the sensor noise, and the system parameter variations. However in nuclear steam generator water level control, fault-tolerant components of interest are controllers and sensors instead of an actuator, because the strategy of duplicating an actuator to increase reliability of the system, is unrealistic in light of cost-benefit effect. The configuration of the passive redundant control system, with no reconfiguration mechanism, consists of single actuator and identical controllers and sensors, shown in Fig. 1. This is motivated by the common practice in nuclear power plant to improve reliability of instrument and control system using identical sensors and controllers.

II. Fault-Tolerant Control

Consider the fault-tolerant control system shown in Fig. 1. Plant is described as a linear time-invariant systems described by state-space equations

$$\begin{aligned} \dot{x} &= Ax + B_1\omega + B_2u \\ z &= C_1x \\ y &= C_2x \end{aligned} \tag{1}$$

where $x \in R^n$ is the state, $u \in R^q$ is the control input, $w \in R^m$ is the disturbance input which belongs to $L_2[0,\infty)$, $z \in R^l$ is the controlled output, $y \in R^r$ is the measured output, and A, B_1, and C_1, are of appropriates dimensions. It is assumed that the pair (A, B_2) and (A, C_2) are stabilizable and detectable, respectively.

Definition 1. **Fault-tolerant**

The controlled system depicted in Fig. 1 is said to be fault-tolerant if the following conditions are satisfied 1) *when both controllers operate simultaneously, the controlled system is stable,* 2) *when only one of controllers is in operation, the controlled system is stable, and* 3) *the controlled system has* H_∞ *norm from the disturbance input to the controlled output less than the positive,* γ.

That is, in the normal mode, both identical controllers C_1 and C_2 are operational and then the closed-loop system is stable. If either controller is fail, it is still stable, even the performance of the closed-loop system might be effected adversely.

III. Fault-Tolerant State-Feedback Control

Consider where both C_1 and C_2 are equivalent state feedback controller, K, respectively, and they are in operation. Then, the total control input, u, is

$$\begin{aligned} u_1 &= K, \\ u_2 &= K, \\ u &= u_1 + u_2 \\ &= 2Kx. \end{aligned} \tag{2}$$

Then the closed-loop system can be written as

$$\begin{aligned} \dot{x} &= Ax + B_1\omega + 2B_2Ku \\ &= (A + 2BK)x + [B_1 \ 0] \begin{bmatrix} \omega \\ u_0 \end{bmatrix} \\ z &= C_1x \\ y &= C_2x. \end{aligned} \tag{3}$$

where u_0 is considered as pseudo-disturbance input signal.

Next where either controller is in operation and the other is in fault. It is assumed that faulty controller gives the output u_0 irrespective of controller input and it belongs to $L_2[0, \infty)$. Here we assume that the intact controller is C_1 and the faulty C_2. That is, the total control input, u, is

$$\begin{aligned} u &= u_1 + u_2 \\ &= u_1 + u_0. \end{aligned} \tag{4}$$

Then the closed-loop system can be described as

$$\begin{aligned}
\dot{x} &= Ax + B_1\omega + B_2u \\
&= Ax + B_1\omega + B_2(u_1 + u_0) \\
&= Ax + [B_1 \ B_2]\begin{bmatrix} \omega \\ u_0 \end{bmatrix} + B_2u_1 \\
z &= C_1x \\
y &= C_2x.
\end{aligned} \tag{5}$$

The fault-tolerant control satisfies both (3) and (5) at the same time. These conditions are equivalent to H_∞ control for uncertain linear time-varying systems with state-space matrices varying in a polytope:

$$\begin{aligned}
\dot{x} &= Ax + \tilde{B}_1\omega + \tilde{B}_2u \\
z &= C_1x \\
y &= C_2x.
\end{aligned} \tag{6}$$

where

$$\begin{aligned}
&(\tilde{B}_1 \quad \tilde{B}_2) \in \text{Co}\,\{(B_{1k} \quad B_{2k}) : k = 1, 2\} \\
&B_{11} = [B_1 \quad B_2],\ B_{12} = [B_1 \quad 0],\ B_{21} = B_2,\ B_{22} = 2B_2.
\end{aligned}$$

Therefore, the problem of finding state feedback controller, K, can be converted into seeking a single quadratic Lyapunov function that enforces the design objectives for all systems in the polytope leads to the following LMIs:

$$\begin{bmatrix} AX_1 + B_{21}L + X_1A^T + L^TB_{21}^T & B_{11} & X_1C_1^T \\ B_{11}^T & -I & 0 \\ C_1X_1 & 0 & -\gamma^2 I \end{bmatrix} < 0 \tag{7}$$

$$\begin{bmatrix} AX_2 + B_{22}L + X_2A^T + L^TB_{22}^T & B_{11} & X_2C_1^T \\ B_{11}^T & -I & 0 \\ C_1X_2 & 0 & -\gamma^2 I \end{bmatrix} < 0 \tag{8}$$

$$\begin{bmatrix} AX_3 + B_{21}L + X_3A^T + L^TB_{21}^T & B_{12} & X_3C_1^T \\ B_{12}^T & -I & 0 \\ C_1X_3 & 0 & -\gamma^2 I \end{bmatrix} < 0 \tag{9}$$

$$\begin{bmatrix} AX_4 + B_{22}L + X_4A^T + L^T B_{22}^T & B_{12} & X_4C_1^T \\ B_{12}^T & -I & 0 \\ C_1X_4 & 0 & -\gamma^2 I \end{bmatrix} < 0. \tag{10}$$

Theorem 1. *The closed-loop system (1) under state-feedback control* $u1 = Kx$, $u2 = Kx$ *is fault-tolerant with disturbance attenuation* γ *if there exists a solution of LMIs (7)* $\sim$ *(10) with a common Lyapunov function,* $X > 0$*. The corresponding state-feedback gain is give by*

$$K = LX^{-1}$$

proof : Let a single Lyapunov function $X := X_1 = X_2 = X_3 = X_4 > 0$ *these conditions of (7)* $\sim$ *(10) are jointly convex in* K *and* X*, but by a simple change of variable,* $L = KX$*, we can obtain an quadratic stabilizability with disturbance attenuation* γ*. Using the realization*

$$\begin{aligned} A_{cl1} &= A + B_{21}K, \quad B_{cl1} = B_{11}, \quad C_{cl1} = C_1, \\ A_{cl2} &= A + B_{22}K, \quad B_{cl2} = B_{11}, \quad C_{cl2} = C_1, \\ A_{cl3} &= A + B_{21}K, \quad B_{cl3} = B_{12}, \quad C_{cl3} = C_1, \\ A_{cl4} &= A + B_{22}K, \quad B_{cl4} = B_{12}, \quad C_{cl4} = C_1 \end{aligned} \tag{11}$$

for the closed-loop system. We can easily obtain the following the H_∞ *constraints which is equivalent the existence of a solution* $X > 0$ *to the LMIs known as the Bounded Real Lemma*

$$\begin{bmatrix} A_{cli}X + XA_{cli}^T & B_{cli} & XC_{cli}^T \\ B_{cli}^T & -I & 0 \\ C_{cli}X & 0 & -\gamma^2 I \end{bmatrix} < 0, i = 1, \ldots, 4. \tag{12}$$

IV. Fault-Tolerant Output-Feedback Control

Our goal can be stated as finding output-feedback controllers, C_1, C_2 such that the energy of the controlled output z is bounded by some prescribed number γ for any input ω under the condition that both controllers are in operation or either controller is in operation while the other in failure. Consider where both C_1 and C_2 are equivalent output feedback controllers.

First consider where both controllers, C_1 and C_2 are in operation. Then total control input, u, is

$$\begin{aligned} u &= u_1 + u_2 \\ &= 2u_1 \\ &= 2u_2. \end{aligned} \tag{13}$$

Then the closed-loop system can be written as

$$\begin{aligned} \dot{x} &= Ax + B_1\omega + B_2u \\ &= Ax + B_1\omega + 2B_2u_1 \\ &= Ax + [B_1\ 0]\begin{bmatrix} \omega \\ u_0 \end{bmatrix} + 2B_2u_1 \\ z &= C_1x \\ y &= C_2x. \end{aligned} \tag{14}$$

where u_0 is considered as pseudo-disturbance input signal.

Next where either controller is in operation and the other is in failure. In the same way, it is assumed that faulty controller gives the output u_0 irrespective of the input of controller and it belongs to $L_2[0,\infty)$. Here we assume that the intact controller is C_1 and the faulty C_2. That is, the total control input, u, is

$$\begin{aligned} u &= u_1 + u_2 \\ &= u_1 + u_0. \end{aligned} \tag{15}$$

Then the closed-loop system can be described as

$$\begin{aligned} \dot{x} &= Ax + B_1\omega + B_2u \\ &= Ax + B_1\omega + B_2(u_1 + u_0) \\ &= Ax + [B_1\ B_2]\begin{bmatrix} \omega \\ u_0 \end{bmatrix} + B_2u_1 \\ z &= C_1x \\ y &= C_2x. \end{aligned} \tag{16}$$

The fault-tolerant control in the sense of H_∞-norm is converted into H_∞ output-feedback control that simultaneously stabilizes two systems, (14), (16) and satisfies the H_∞ norm from the system disturbance to the controlled output signal. This is equivalent to H_∞ output-feedback control for uncertain linear time invariant systems.

$$\begin{aligned} \dot{x} &= Ax + [\tilde{B}_1 \ \Delta B_1] \begin{bmatrix} \omega \\ u_0 \end{bmatrix} + [\tilde{B}_2 \ \Delta B_2]u \\ z &= C_1 x \\ y &= C_2 x. \end{aligned} \tag{17}$$

where,

$$\tilde{B}_1 = \begin{bmatrix} B_1 & \frac{1}{2}B_2 \end{bmatrix}, \quad \tilde{B}_2 = \frac{3}{2}B_2.$$

The uncertainties will be assumed in the form

$$\begin{bmatrix} \Delta B_1 & \Delta B_2 \end{bmatrix} = HF(t) \begin{bmatrix} E_1 & E_2 \end{bmatrix}.$$

where $F(t) \in R^{i \times j}$ is an unknown matrix satisfying $F(t)^T F(t) \leq I$ and H, E_1, E_2 are known matrices of appropriate dimensions. In this analysis, $H = B_2$, $F(t) = I$, $E_1 = [0 \ \ \frac{1}{2}I]$, and $E_2 = \frac{1}{2}I$.

We now introduce the system below that will allow us to establish the equivalence between robust H_∞ systems and uncertainty free control systems in the sense of H_∞-norm.

$$\begin{aligned} \dot{x} &= Ax + [\tilde{B}_1 \ \gamma\lambda H] \begin{bmatrix} \omega \\ u_0 \\ \tilde{\omega} \end{bmatrix} + \tilde{B}_2 u \\ \begin{bmatrix} z \\ \tilde{z} \end{bmatrix} &= \begin{bmatrix} C_1 \\ 0 \end{bmatrix} x + \begin{bmatrix} 0 & 0 \\ \frac{1}{\lambda}E_1 & 0 \end{bmatrix} \begin{bmatrix} \omega \\ u_0 \\ \tilde{\omega} \end{bmatrix} + \begin{bmatrix} 0 \\ \frac{1}{\lambda}E_2 \end{bmatrix} u \\ y &= C_2 x. \end{aligned} \tag{18}$$

with u the control input, $[\omega, \ u_0, \ \tilde{\omega}]^T$ the exogenous input, y measured output and $[z, \ \tilde{z}]^T$ regulated output.

Theorem 2. *There exists fault-tolerant controller with γ disturbance attenuation for the system (1) of structure is shown in Fig.1, if there exists a $\lambda > 0$ such that the systems (18) can be stabilized with its H_∞ norm less than γ by an output feedback control.*

proof : In the sense of H_∞-norm the system (18) is equivalent to uncertain LTI system (17) of which uncertainties are introduced to present fault-tolerant conditions, shown in [7]. If the output feedback controller $u = Ky$ satisfies H_∞ norm performance of (18), it achieves fault-tolerant conditions for original system (1).

V. Simulations

This section shows the application of the fault-tolerant synthesis technique to the control of the nuclear steam generator of Irving's steam generator model [8] at 100% power level. The fault-tolerant control system has passive redundant structure consisting of dual controllers, sensors and feedforward compensator. The input of controller is only the deviation from the prescribed water level. The feedforwad compensator is involved, of which input is the deviation from nominal steam flow rate, to improve performance of the controlled system.

The fault-tolerant controller, K(s), is obtained as

$$K(s) = \frac{-12.55s^4 - 16.94s^3 - 84.21s^2 - 51.63s - 11.3}{1. \times 10^{-4}s^5 + 0.05s^4 + 1.6s^3 + 2.22s^2 + 1.1s + 1.75}$$

The controller C_1 is fail-zero at $110sec$, shown in Fig. 2, the intact controller C_2 works properly, resulting that the water level goes to stable level after $200sec$. Fig. 3 illustrates the responses of the steam generator in case of controller C_1 fail-low. When it fails low, the controller C_1 compensates the fault signal so the water level settles down at about $200mm$. That is, fault-tolerant controller prevents the plant from tripping. Fig. 4 shows that the controller C_1 fails at $100sec$, the controller C_2 properly controls water level, resulting in no reactor trip. Where the fault controller channel is defeated at $200sec$, the final water level goes to normal state. The feedforward compensator under fail-low situation is simulated, as other situations, dual controllers compensate the fault signal of feedforward, resulting the controlled system become stable with about $200mm$ level deviation, shown in Fig. 5. Finally, Fig. 6 shows the performance test of both the proposed controller and PID controller under without faults. It is showm that the proposed fault-tolerant controller has fast responses that the PID controller does.

VI. Conclusions

In this paper it has been described that the fault-tolerant control design methodologies to guarantee both stability and H_∞ disturbance attenuation, not only when the system is operating properly, but also when the system fails. The designs are implemented by including additional disturbance inputs and regulated outputs to present possible controller faults in the nominal plant, and then by applying the H_∞ control theory for the augmented system. Also the existence conditions in terms of LMIs for this augmented system are derived for state-feedback and output-feedback control. The performance of the proposed controller is tested with Irving's steam generator model. The simulations show that the fault-tolerant controller has proven to be robust whether the controller fail or not. Moreover, in comparison to the conventional PID controller, it performs even better with respect to step response.

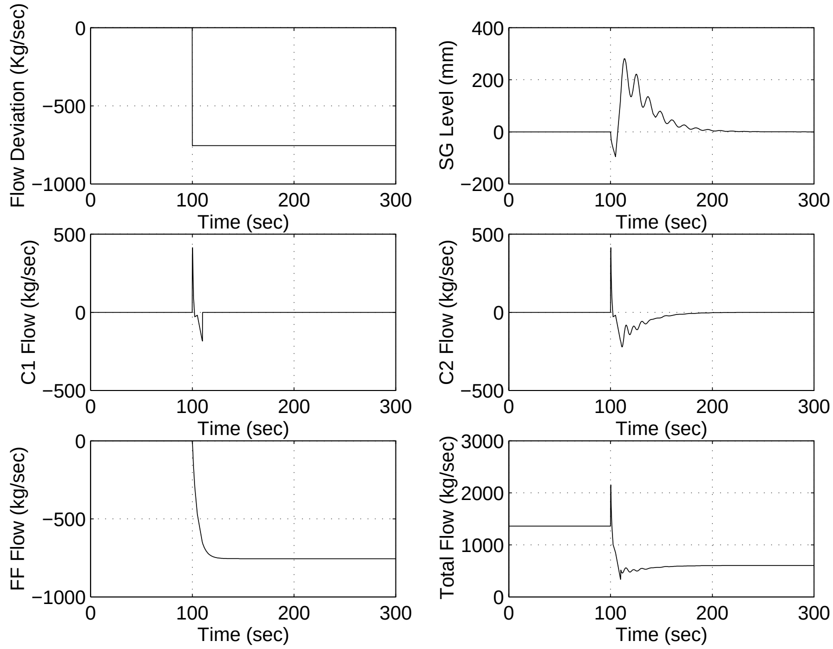

Fig. 2. Responses of fault-tolerant controller at 100% power in case of controller C_2 fail-zero: flow deviation (a), water level (b), controller C_1 output (c), controller C_2 output (d), feedforward compensator output (e) and total controller output (f).

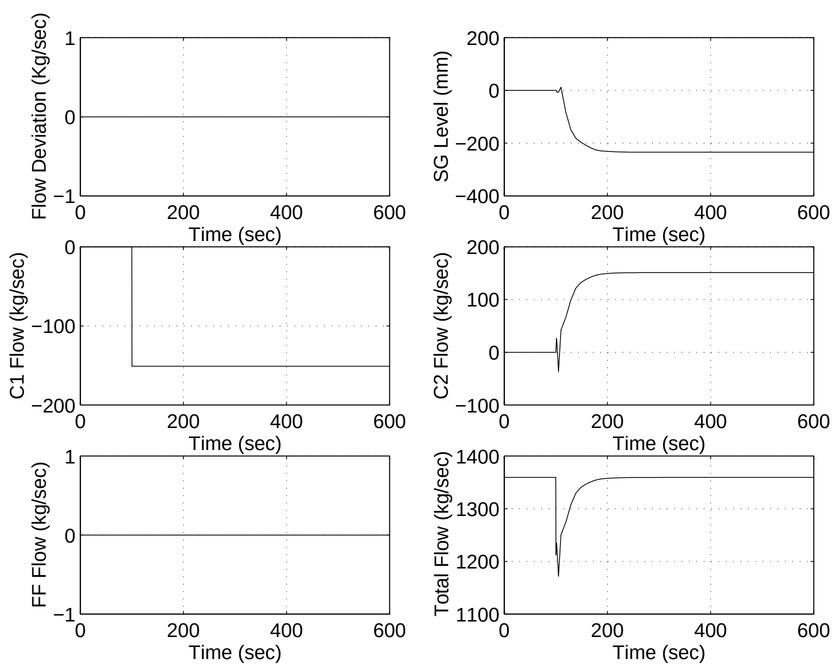

Fig. 3. Responses of fault-tolerant controller at 100% power in case of controller C_2 fail-low: flow deviation (a), water level (b), controller C_1 output (c), controller C_2 output (d), feedforward compensator output (e) and total controller output (f).

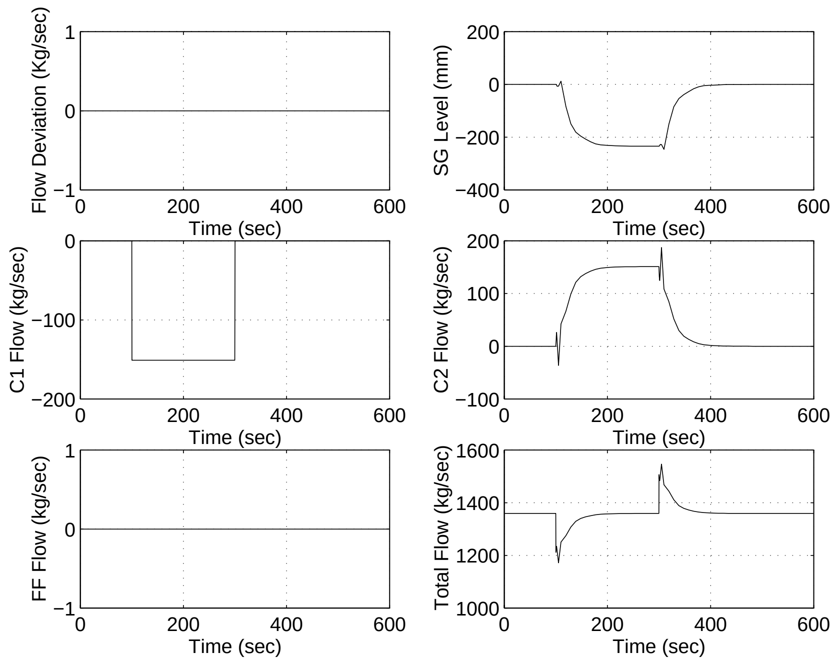

Fig. 4. Responses of fault-tolerant controller at 100% power in case of controller C_2 fails at 100sec and defeated at 200sec : flow deviation (a), water level (b), controller C_1 output (c), controller C_2 output (d), feedforward compensator output (e) and total controller output (f).

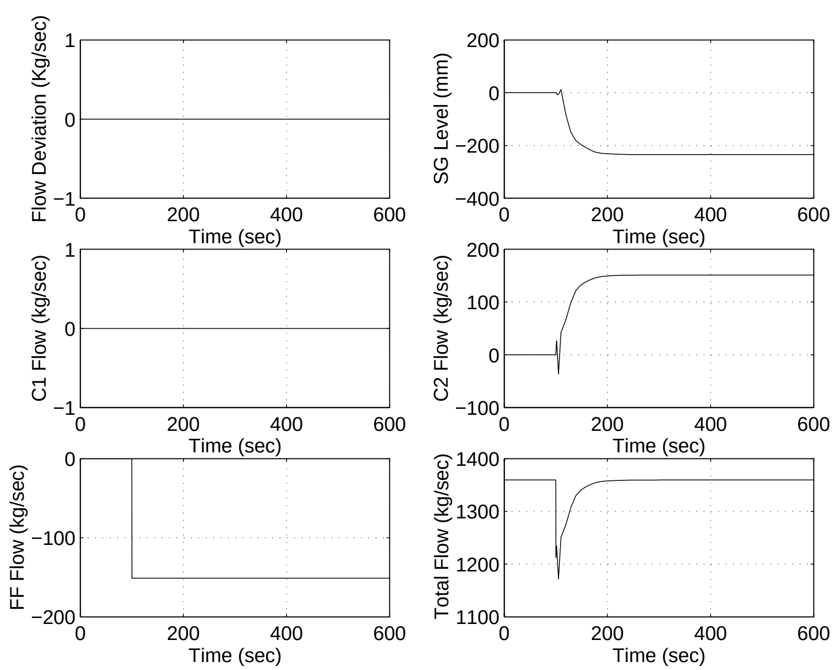

Fig. 5. Responses of fault-tolerant controller at 100% power in case of feedforward compensator fail-low: flow deviation (a), water level (b), controller C_1 output (c), controller C_2 output (d), feedforward compensator output (e) and total controller output (f).

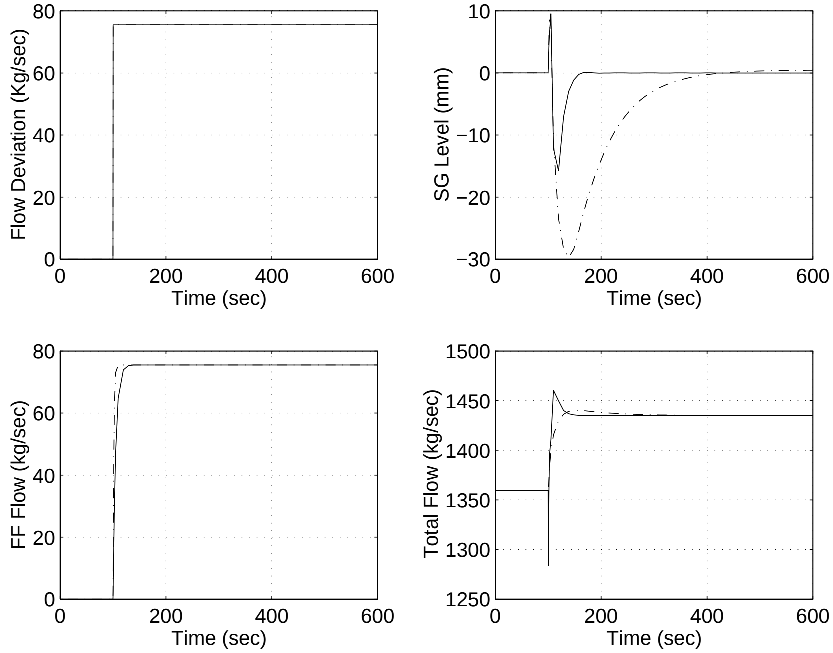

Fig. 6. Responses of fault-tolerant controller(–) and PID (-·) at 100% power: flow deviation (a), water level (b), feedforward flow rate (c), total flow rate (d).

References

[1] R. Isermann, "Process fault detection based on modeling and estimation methods - A survey," *Automatica*, vol. 20, pp. 387–404, 1984.

[2] M. S. Phatak, N. Viswanadham, "Actuator fault detection and isolation in linear systems," *Int. J. Sys. Sci.*, vol. 19, no. 12, pp. 2593–2603, 1988.

[3] P. M. Frank, "Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy - A survey and some new results," *Automatica*, vol. 26, no. 3, pp. 459–474, 1990.

[4] M., Vidyasagar, and N. Viswanadham, "Reliable stabilization using a multi-controller configuration," *Automatica*, vol. 21, no. 5, pp. 599–602, 1985.

[5] J. R. Veillette, V. J. Medanic, R. W. Perkins, "Design of reliable control systems," *IEEE Trans, Auto. Control*, vol. AC-37, no. 3, pp. 290–304, 1992.

[6] C. Seo, "A study on robust and reliable H_∞ control for uncertain linear systems," Ph.D. dissertaiton, KAIST, Korea, 1995.

[7] K. Gu, " H_∞ control of systems under norm bounded uncertainty in all system matrices," *IEEE Trans, Auto. Control*, vol. 39, no. 6, pp. 1320–1322, 1992.

[8] E. Irving, C. Miossec, and J. Tassart, "Towards efficient full automatic operation of the PWR steam generator with water level adaptive control," in *Proc. 2nd Conf. Boiler dynamics and control in nuclear power station*, Bournemouth, U.K., 1979, pp. 309 – 329.

(a) (b) (c) (d) (e) (f) (a) (b) (c) (d) (e) (f) (a) (b) (c) (d) (e) (f) (a) (b) (c) (d) (e) (f)