2013 European Control Conference (ECC)
July 17-19, 2013, Zürich, Switzerland.

Fault-tolerant servo systems against sensor failures using limited integrators

Koichi Suyama
Tokyo University of Marine Science and Technology
Etchujima, Koto-ku, Tokyo 135-8533, Japan
suyama@kaiyodai.ac.jp

Noboru Sebe
Kyushu Institute of Technology
Kawazu, Iizuka, Fukuoka 820-8502, Japan
sebe@ai.kyutech.ac.jp

Abstract— **No effective controller design for achieving the tolerance against sensor failures has been proposed for servo systems until now because it is difficult to deal with ramp signals generated by integrators in the servo performance. In this paper, we obtain a key for the limiting function in limited integrators to behave effectively as the measure against ramp signals for the first time. Then, the limiting function and a controller can be designed in a unified framework of simultaneous optimization with consideration given to the servo performance in the normal case and in faulty cases. The obtained result succeeds in establishing the potential applicability of limited integrators to fault-tolerant servo systems.**

I. Introduction

The social environment surrounding system safety has changed rapidly, and then safety measures are now required for the various kinds of control systems operating in various situations. Although it is needless to say that in almost all application areas of control theory, servomechanism [1] is one of the most important control technologies, servo systems are no exception. From a viewpoint of risk reduction required by international standards, such as IEC 61508 [2], especially the safety measures against failures in sensors and actuators are important.

Over the past few decades, several studies have been made on controller design to achieve the tolerance against failures in actuators and/or sensors without their detection/isolation, e.g., integrity [3], reliable H_∞ control [4], robust and reliable H_∞ control [5], a simultaneous stabilization approach [6], and multiobjective design using the switching L_2 gain for the safety against deviations [7]. In such an approach, we presented fault-tolerant servo systems against actuator failures in [8]. However, to the best of our knowledge, no effective methods for achieving the tolerance against sensor failures in servo systems have been proposed until now, especially in such an approach. (For example, the theory of integral-action integrity [9] does not aim at achieving the tolerance against sensor failures.) The main reason is that it is difficult to deal with ramp signals caused by sensor failures with consideration given to the servo performance of the overall control systems.

It may be misunderstood that the combined use of limited integrators and a simultaneously stabilizing controller is one of possible measures against sensor failures in servo systems because the limiting function implemented in integrators can superficially cut off ramp signals caused by sensor failures. However, even if we use a simultaneously stabilizing controller for the normal case and faulty cases, the limiting function does not always behave effectively as the measure against sensor failures. It is because the limiting function can causes unintended saturations, which lead to poor servo performance or system instability.

In this paper, we obtain a key for the limiting function to behave effectively as the measure against ramp signals caused by sensor failures for the first time. Then, the limiting function and a controller can be designed in a unified framework of simultaneous optimization with consideration given to the servo performance in the normal case and in faulty cases. The obtained result is very useful for potential applications of limited integrators to fault-tolerant servo systems.

For simplicity, we discuss fault-tolerant servo systems against sensor failures for two-input two-output plants in this paper. We can easily extend the discussion to the m-input m-output plant case.

The following notations are used in this paper. $\mathbb{R}$: the field of real numbers, I: an identity matrix of appropriate dimensions, A^{T}: the transpose of a matrix A, T_{zw}: the transfer function matrix from a signal w to another z, and $\|G\|_\infty$: the H_∞ norm of a transfer function matrix G.

II. Problem statement

A. Servo system

Figure 1 shows the general configuration of servo systems, where P is a two-input two-output plant and K is a controller. Here, $r(t) = \begin{bmatrix} r_1(t) & r_2(t) \end{bmatrix}^{\mathrm{T}} \in \mathbb{R}^2$ is the reference signals; $v(t) = \begin{bmatrix} v_1(t) & v_2(t) \end{bmatrix}^{\mathrm{T}} \in \mathbb{R}^2$ is the outputs of integrators; $u_1(t), u_2(t) \in \mathbb{R}$ are the control inputs; $y_1(t), y_2(t) \in \mathbb{R}$ are the measured outputs; $n_1(t), n_2(t) \in \mathbb{R}$ are the sensor noises; $\hat{y}_1(t), \hat{y}_2(t) \in \mathbb{R}$ are the measured values of the outputs. The $W_1(s)$ and $W_2(s)$ are the weighting functions for evaluating the servo performance; $z(t) = \begin{bmatrix} z_1(t) & z_2(t) \end{bmatrix}^{\mathrm{T}} \in \mathbb{R}^2$ is the evaluated outputs. Let Loop i $(i = 1,2)$ denote the control loop with Integrator i. It includes v_i, u_i, y_i, and $\hat{y}_i$ as well as its reference input r_i.

1) Plant: The plant P is finite-dimensional, linear, and time-invariant. We assume the following:

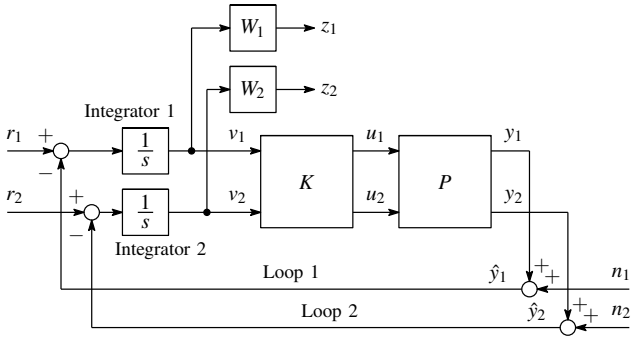

Fig. 1. Servo system in the normal case.

Assumption 2.1:
(i) The plant P is stabilizable and detectable by both Loops 1 and 2, by Loop 1 individually, and by Loop 2 individually.
(ii) The plant P is simultaneously stabilizable by both Loops 1 and 2, by Loop 1 individually, and by Loop 2 individually.

2) Integrators: Both Integrators 1 and 2 in Fig. 1 are limited ones, such as a "Integrator Limited block" in `SIMULINK`. If the output $v_i(t)$ of Integrator i reaches the upper limit $\ell_i\,(>0)$ or lower limit $-\ell_i$ at $t=t_0$, the integral action is turned off. Then, $v_i(t)$ is saturated at the upper/lower limit. This is the limiting function implemented in the integrators. Of course, when the integral value is situated between the limits, the output v_i is the value itself.

Strictly speaking, Fig. 1 shows the servo system in the normal case under the condition that both outputs of Integrators 1 and 2 are not saturated by the limiting function.

3) Reference signals: For simplicity, we assume the following on the reference signals:

Assumption 2.2:
(i) The reference signal $r_i(t)\ (i=1,2)$ is a stepped one

$$r_i(t)=r_{ij}, \qquad t_{ij}\le t<t_{i(j+1)} \tag{1}$$

where r_{ij} is a real constant, $j=1,2,\ldots$, and $0=t_{i1}<t_{i2}<\cdots$.
(ii) The reference signal $r_i(t)\ (i=1,2)$ is limited as

$$-\bar{r}_i\le r_i(t)\le\bar{r}_i, \qquad t\ge 0, \tag{2}$$

where $\bar{r}_i\,(>0)$ is known ahead of time.
This assumption implies that

$$-\bar{r}_i\le r_{ij}\le\bar{r}_i, \qquad i=1,2 \ \text{ and } \ j=1,2,\ldots. \tag{3}$$

4) Sensor noises: We assume the following on the sensor noises:

Assumption 2.3:

$$n_i(t)=0, \qquad t\ge 0 \ \text{ and } \ i=1,2. \tag{4}$$

Remark 2.4: In this paper, we focus on a ramp signal immediately after a sensor failure generated by the integrator. Thus, we consider Assumption 2.3 so that a ramp signal actually appears as (7) below. However, in the discussion of the measures against sensor failures proposed in this paper, the essence of sensor failures is that if Sensor $i\ (i=1,2)$ fails at $t=t_0\,(>0)$, there exist constants $t=t_0'\ (t_0<t_0'<\infty)$ and $M_i\ (|M_i|<\infty)$ such that

$$v_i(t)=M_i, \qquad t\ge t_0'. \tag{5}$$

Thus, we can loosen Assumption 2.3. That is, the sensor noise $n_i\ (i=1,2)$ is enough to satisfy $|n_i(t)|\le\bar{n}_i\,(\ll\bar{r}_i)$, which does not prevent $v_i(t)$ from reaching the upper/lower limit and being saturated by the limiting function. For example, in the simulation in Section IV, we assume that n_i is a white Gaussian noise generated by the normal distribution $N(\mu,\sigma^2)$ with appropriate saturation limits, where μ and σ^2 are the mean and variance, respectively.

B. Sensor failures

In Fig. 1, y_1 and y_2 are measured by Sensors 1 and 2, respectively. In this paper, we consider the following failure mode of the sensors:

Assumption 2.5: Under Assumption 2.3, if Sensor $i\ (i=1,2)$ fails at $t=t_0$, its output becomes

$$\hat{y}_i(t)=\hat{y}_{i0}\,(=\text{const.}), \qquad t\ge t_0, \tag{6}$$

where $\hat{y}_{i0}$ is finite and independent of any other signals in the servo system including the measured output $y_i(t)$.
A loop with a failed sensor is referred as a "failed loop." On the contrary, a loop with a normally-functioning sensor is referred as a "normal loop." Then, in addition, we assume the following:

Assumption 2.6: The reference signal into a failed loop is never changed.

Suppose that Sensor $i\ (i=1,2)$ fails at $t=t_0\,(>0)$. Then, under Assumptions 2.5 and 2.6, the output of Integrator i after the failure is as follows:

$$v_i(t)=\begin{cases}(r_{i0}-\hat{y}_i)(t-t_0)+v_i(t_0), & t_0<t<t_0'\\ \ell_i \text{ or } -\ell_i\ (=\text{const.}), & t_0'\le t,\end{cases} \tag{7}$$

where $r_{i0}=r_i(t_0)$ and $t_0'\ (t_0<t_0'<\infty)$ is given by

$$t_0'=\max\left\{t'\,\middle|\,|v_i(t')|<\ell_i,\ \forall t<t'\right\}. \tag{8}$$

(In the general case where $r_{i0}\ne\hat{y}_i$, there exists such a time t_0' when $v_i(t)$ reaches the upper limit ℓ_i or lower limit $-\ell_i$.) That is, the output of the integrator on a failed loop is a ramp signal immediately after the failure. However, due to the limiting function implemented in the integrator, it is saturated at the upper/lower limit after it reaches the limit. (On the other hand, if $r_{i0}=\hat{y}_i$, then $v_i(t)=v_i(t_0)\ (t>t_0)$, which is finite and constant.)

Remark 2.7: Due to the same reason as Remark 2.4, we consider Assumptions 2.5 and 2.6. Thus, we can loosen them as well as Assumption 2.3. That is, in Assumption 2.5, the measured value $\hat{y}_i(t)$ by the failed Sensor i is enough to be finite and independent of the plant output $y_i(t)$ which does not prevent $v_i(t)$ from reaching the upper/lower limit and being saturated by the limiting function. Also in Assumption 2.6, it is sufficient that the reference signal into a loop with an integrator whose output is saturated by the limiting function is never changed.

C. Design problem

The design problem considered in this paper is summarized below.

(i) Given:

- Plant P
- Weighting functions for evaluating the servo performance: W_1 and W_2
- Range of the reference signal: $\bar{r}_1$ and $\bar{r}_2$.

(ii) Fault-tolerant servo system to be achieved: Even if either of Sensors 1 and 2 fails, the overall system maintains the stability and a normal loop maintains an acceptable servo performance. (We will discuss concrete design requirements in the subsequent section.)

(iii) To be designed:

- Controller K
- Limits ℓ_1 and ℓ_2 of the limiting functions implemented in Integrators 1 and 2, respectively.

III. Fault-tolerant servo system design

A. Normal case

Consider the servo system in the normal case where both sensors function normally as shown in Fig. 1. Note that Fig. 1 is subject to the condition that both outputs of Integrators 1 and 2 are not saturated by the limiting function.

1) Performance requirement: Under the stability of the overall servo system, we consider the requirement for the normal-case servo performance by

$$\|T_{zr}\|_\infty < \gamma_{\rm d}, \tag{9}$$

where $\gamma_{\rm d}$ denotes a desirable performance level in the normal case.

2) Requirements for the limits: In addition, we must consider the requirement for the situation where both outputs of Integrators 1 and 2, $v_1(t)$ and $v_2(t)$, are not saturated by the limiting function.

In Fig. 1, we have

$$T_{vr} = (sI + PK)^{-1}. \tag{10}$$

Thus, the steady-state value of $v(t)$ corresponding to $r(t) = \begin{bmatrix} r_{1j_1} & r_{2j_2} \end{bmatrix}^{\rm T}$ is obtained by

$$\big(P(0)K(0)\big)^{-1} \begin{bmatrix} r_{1j_1} \\ r_{2j_2} \end{bmatrix}. \tag{11}$$

Using (3) and considering possible overshoots of transient responses in $v_1(t)$ and $v_2(t)$, sensor noises, and the model error in P, we have that the following inequalities must hold with appropriate margins:

$$\big(\eta_1 = \big)\frac{1}{\ell_1} \cdot \max_{\substack{r_1=\pm\bar{r}_1 \\ r_2=\pm\bar{r}_2}} \left| \begin{bmatrix} 1 & 0 \end{bmatrix} \big(P(0)K(0)\big)^{-1} \begin{bmatrix} r_1 \\ r_2 \end{bmatrix} \right| < 1 \tag{12}$$

$$\big(\eta_2 = \big)\frac{1}{\ell_2} \cdot \max_{\substack{r_1=\pm\bar{r}_1 \\ r_2=\pm\bar{r}_2}} \left| \begin{bmatrix} 0 & 1 \end{bmatrix} \big(P(0)K(0)\big)^{-1} \begin{bmatrix} r_1 \\ r_2 \end{bmatrix} \right| < 1. \tag{13}$$

These are the requirements for the limits in the normal case.

B. Sensor 1 fault case

Figure 2 shows the servo system in the case where Sensor 1 is in a fault and Sensor 2 functions normally. Although $v_1(t)$ is described as an exogenous input, it is supposed to be equivalent to the output of Integrator 1 given in (7). Note that Fig. 2 is subject to the condition that $v_2(t)$ on the normal Loop 2 is not saturated by the limiting function implemented in Integrator 2.

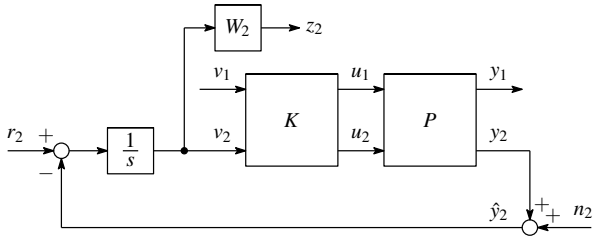

Fig. 2. Servo system in Sensor 1 fault case.

1) Performance requirement: Under the stability of the servo system shown in Fig. 2, we consider the requirement for the servo performance of the normal Loop 2 by

$$\|T_{z_2 r_2}\|_\infty < \gamma_{2\rm a}, \tag{14}$$

where $\gamma_{2\rm a}$ denotes an acceptable performance for Loop 2 in the Sensor 1 fault case. This is the measures against possible changes in the reference signal into the normal loop after a sensor failure (see Assumption 2.6). By this servo performance, the effect of the output of an integrator on a failed loop saturated by the limiting function on another normal loop can be eliminated as a constant disturbance.

2) Requirements for the limiting function: In Fig. 2, immediately after a failure in Sensor 1, $v_2(t)$ is also a ramp signal by the effect of $v_1(t)$ given in (7). Thus, for the condition that only $v_1(t)$ is saturated by the limiting function, we should consider the following:

(a) $v_1(t)$ reaches the upper/lower limit, ℓ_1 or $-\ell_1$, sufficiently early, and

(b) the steady-state value of $v_2(t)$ against $v_1(t) = \pm\ell_1$ is situated between the limits $\pm\ell_2$.

For simplicity of description, define L_{11}, L_{12}, L_{21}, and L_{22} by

$$\begin{bmatrix} L_{11} & L_{12} \\ L_{21} & L_{22} \end{bmatrix} = PK. \tag{15}$$

(a): Let the gradients of the ramp signals in $v_1(t)$ and $v_2(t)$ immediately after a failure in Sensor 1 denote β_1 and β_2, respectively. In Fig. 2, we have

$$\beta_2 = T_{v_2 v_1}(0)\beta_1. \tag{16}$$

Thus, if it holds with a sufficient margin that

$$|T_{v_2 v_1}(0)| < 1, \tag{17}$$

$|\beta_1|$ is sufficiently larger than $|\beta_2|$. That is, $v_1(t)$ approaches the upper/lower limit at a sufficiently faster speed than $v_2(t)$.

Then, $v_1(t)$ reaches the upper/lower limit sufficiently earlier than $v_2(t)$.

(b): In Fig. 2, we have

$$T_{v_2v_1} = -(s+L_{22})^{-1}L_{21} \tag{18}$$

$$T_{v_2r_2} = (s+L_{22})^{-1}. \tag{19}$$

Thus, the steady-state value of $v_2(t)$ corresponding to $v_1(t) = \pm\ell_1$ and $r(t) = r_{2j}(=\text{const.})$ is obtained by

$$-L_{22}^{-1}(0)L_{21}(0)\,\ell + L_{22}^{-1}(0)\,r_{2j}, \tag{20}$$

where $\ell = \pm\ell_1$. Thus, if it holds with a sufficient margin that

$$(\xi_2 =)\ \frac{|L_{22}^{-1}(0)L_{21}(0)|\,\ell_1 + |L_{22}^{-1}(0)|\,\bar{r}_2}{\ell_2} < 1, \tag{21}$$

the steady-state value of $v_2(t)$ against $v_1(t) = \pm\ell_1$ is situated between the limits $\pm\ell_2$.

C. Sensor 2 fault case

Figure 3 shows the servo system in the case where Sensor 2 is in a fault and Sensor 1 functions normally. Although $v_2(t)$ is described as an exogenous input, it is supposed to be equivalent to the output of Integrator 2 given in (7). Note that Fig. 3 is subject to the condition that $v_1(t)$ is not saturated by the limiting function.

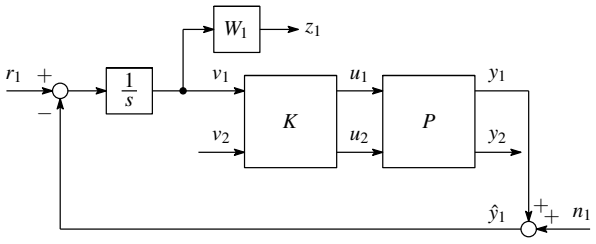

Fig. 3. Servo system in Sensor 2 fault case.

The discussion in this case is entirely analogous to that in the case where Sensor 1 is in a fault in Section III-B. Thus, we present only requirements.

1) Performance requirement: Under the stability of the servo system shown in Fig. 3, we consider the requirement for the servo performance of the normal Loop 1 by

$$\|T_{z_1r_1}\|_\infty < \gamma_{1a}, \tag{22}$$

where γ_{1a} denotes an acceptable performance for Loop 1 in the Sensor 2 fault case.

2) Requirements for the limiting function: (a): In Fig. 3, if it holds with a sufficient margin that

$$|T_{v_1v_2}(0)| < 1, \tag{23}$$

$v_2(t)$ approaches the upper/lower limit at a sufficiently faster speed than $v_1(t)$. Then, $v_2(t)$ reaches the upper/lower limit sufficiently earlier than $v_1(t)$.

(b): If it holds with a sufficient margin that

$$(\xi_1 =)\ \frac{|L_{11}^{-1}(0)L_{12}(0)|\,\ell_2 + |L_{11}^{-1}(0)|\,\bar{r}_1}{\ell_1} < 1, \tag{24}$$

the steady-state value of $v_1(t)$ against $v_2(t) = \pm\ell_2$ is situated between the limits $\pm\ell_1$.

D. Key for the limiting function

If we choose ℓ_1 and ℓ_2 sufficiently large, the conditions (12) and (13) can be satisfied. However, there do not always exist ℓ_1 and ℓ_2 satisfying the conditions (21) and (24).

From (21) and (24), we have

$$\begin{aligned}&\left[1 - |L_{11}^{-1}(0)L_{12}(0)| \cdot |L_{22}^{-1}(0)L_{21}(0)|\right]\ell_1 \\ &\quad > |L_{11}^{-1}(0)|\,\bar{r}_1 + |L_{11}^{-1}(0)L_{12}(0)| \cdot |L_{22}^{-1}(0)|\,\bar{r}_2\,(>0)\end{aligned} \tag{25}$$

and

$$\begin{aligned}&\left[1 - |L_{11}^{-1}(0)L_{12}(0)| \cdot |L_{22}^{-1}(0)L_{21}(0)|\right]\ell_2 \\ &\quad > |L_{22}^{-1}(0)L_{21}(0)| \cdot |L_{11}^{-1}(0)|\,\bar{r}_1 + |L_{22}^{-1}(0)|\,\bar{r}_2\,(>0).\end{aligned} \tag{26}$$

Here, from (18), we have $T_{v_2v_1}(0) = -L_{22}^{-1}(0)L_{21}(0)$ in Fig. 2. In Fig. 3, we also have $T_{v_1v_2}(0) = -L_{11}^{-1}(0)L_{12}(0)$ in an entirely analogous fashion. Thus, if the conditions (17) and (23) are satisfied, $1 - |L_{11}^{-1}(0)L_{12}(0)| \cdot |L_{22}^{-1}(0)L_{21}(0)| > 0$ in (25) and (26). Then, there exist $\ell_1\,(>0)$ and $\ell_2\,(>0)$ satisfying (21) and (24). That is, it suffices to take ℓ_1 and ℓ_2 sufficiently large as

$$\begin{aligned}\ell_1 > &\left[1 - |T_{v_1v_2}(0)| \cdot |T_{v_2v_1}(0)|\right]^{-1} \\ &\times \left[|L_{11}^{-1}(0)|\,\bar{r}_1 + |T_{v_1v_2}(0)| \cdot |L_{22}^{-1}(0)|\,\bar{r}_2\right]\end{aligned} \tag{27}$$

$$\begin{aligned}\ell_2 > &\left[1 - |T_{v_1v_2}(0)| \cdot |T_{v_2v_1}(0)|\right]^{-1} \\ &\times \left[|T_{v_2v_1}(0)| \cdot |L_{11}^{-1}(0)|\,\bar{r}_1 + |L_{22}^{-1}(0)|\,\bar{r}_2\right].\end{aligned} \tag{28}$$

If we choose ℓ_1 and ℓ_2 sufficiently large, the conditions (12) and (13) can be satisfied. Thus, it is clear that (21) and (24) are the existence condition of the limits ℓ_1 and ℓ_2 such that the limiting function behaves effectively as the measure against sensor failures in servo systems.

Furthermore, from a viewpoint of suppressing the fluctuation of transient responses after a sensor failure, it is desirable that the output of an integrator on a failed loop reaches the upper/lower limit as early as possible. That is, smaller values of ℓ_1 and ℓ_2 are more preferable. On the other hand, it follows from (27) and (28) that the smaller $|T_{v_2v_1}(0)|$ and $|T_{v_1v_2}(0)|$, the smaller ℓ_1 and ℓ_2 satisfying (21) and (24) we can choose. Thus, smaller values of $|T_{v_2v_1}(0)|$ and $|T_{v_1v_2}(0)|$ are more preferable. We can easily understand that decoupling control is one of effective measures against sensor failures because it is the ultimate form of making the values of $|T_{v_2v_1}(0)|$ and $|T_{v_1v_2}(0)|$ small.

In essence, the conditions (17) and (23) are the minimum requirements. Furthermore, the values of $|T_{v_2v_1}(0)|$ and $|T_{v_1v_2}(0)|$ are important for the limiting function to behave effectively as the measure against ramp signals. The performance of fault-tolerant servo systems using limited integrators is predicated upon these key values.

E. Summary of design

The fault-tolerant servo system design proposed in this paper is summarized below.

(i) Controller K: Under the stability of the servo system shown in Figs. 1, 2, and 3, we should design a controller K satisfying

- (9) in Fig. 1
- (14) and (17) in Fig. 2
- (22) and (23) in Fig. 3.

Replacing the conditions (17) and (23) by $\|T_{v_2v_1}\|_\infty < \gamma_{1\ell}$ and $\|T_{v_1v_2}\|_\infty < \gamma_{2\ell}$ ($\gamma_{1\ell}, \gamma_{2\ell} < 1$), respectively, we can reduce such simultaneous optimization to multiobjective design as in [7]. That is, we can consider the following problem:

$$\begin{aligned} \underset{K}{\text{minimize}}\ & \|T_{zr}\|_\infty \\ \text{subject to}\ & \|T_{z_2r_2}\|_\infty < \gamma_{2a},\ \|T_{z_1r_1}\|_\infty < \gamma_{1a}, \\ & \|T_{v_2v_1}\|_\infty < \gamma_{1\ell},\ \|T_{v_1v_2}\|_\infty < \gamma_{2\ell}. \end{aligned} \tag{29}$$

Then, applying the iterative performance improvement procedure using a non-common Lyapunov function presented in [10], we can obtain a controller K.

(ii) Limits ℓ_1 and ℓ_2 of the limiting function implemented in the integrators: Using K obtained in (i), we can obtain ℓ_1 and ℓ_2 satisfying (12), (13), (21), and (24) with appropriate margins against possible overshoots of transient responses in $v_1(t)$ and $v_2(t)$, sensor noises, and the model error in P. Here, from a viewpoint of suppressing the fluctuation of transient responses after a sensor failure, it is desirable that the values of ℓ_1 and ℓ_2 are taken as small as possible.

IV. Example

(i) Given:

(a) Plant:

$$P = \left[\begin{array}{cccc|cc} -4 & -2 & -2 & 2 & 1 & 0 \\ 2 & -4 & -1 & 2 & 0 & -1 \\ 1 & -3 & -4 & 3 & 1 & 1 \\ 2 & 0 & -1 & -2 & -2 & 1 \\ \hline 1 & 2 & -1 & 0 & 0 & 0 \\ 1 & -1 & 1 & 1 & 0 & 0 \end{array}\right]. \tag{30}$$

(b) Weighting functions:

$$W_1 = W_2 = 1 + 0.5s. \tag{31}$$

(c) Range of the reference signals:

$$\bar{r}_1 = \bar{r}_2 = 1. \tag{32}$$

(ii) Controller: We obtained the following:

$$K = \left[\begin{array}{cccc} -4.525 & -0.004 & 1.583 & -3.109 \\ -0.135 & -6.422 & -2.296 & -2.126 \\ 3.064 & 3.646 & -17.794 & 1.986 \\ -3.747 & -3.543 & 2.659 & -26.172 \\ -1.624 & -1.620 & 28.671 & 27.078 \\ -797.408 & -680.317 & 2349.799 & -2644.883 \\ \hline -0.022 & 0.026 & 0.057 & -0.063 \\ 0.007 & 0.002 & -0.073 & -0.132 \end{array}\right.$$
$$\left.\begin{array}{cc|cc} 0.594 & 109.284 & -6.564 & -7.834 \\ -0.874 & -99.827 & -3.956 & -4.313 \\ 4.893 & -59.287 & 3.231 & 27.362 \\ 5.358 & 35.892 & -34.624 & -7.377 \\ -30.415 & -4.036 & 39.360 & -51.040 \\ -410.558 & -2305.954 & -3797.615 & -4710.321 \\ \hline 0.119 & 66.217 & 0 & 0 \\ -1.781 & -1.098 & 0 & 0 \end{array}\right]. \tag{33}$$

This controller gives the following performance:

(a) Normal case:

$$\|T_{zr}\|_\infty = 0.707. \tag{34}$$

(b) Sensor 1 fault case:

$$\|T_{z_2r_2}\|_\infty = 0.646, \qquad |T_{v_2v_1}(0)| = 0.0195. \tag{35}$$

(c) Sensor 2 fault case:

$$\|T_{z_1r_1}\|_\infty = 0.674, \qquad |T_{v_1v_2}(0)| = 0.215. \tag{36}$$

The minimum requirements for the limiting function, (17) and (23), are satisfied with sufficient margins.

(iii) Limiting function: Considering $\eta_1 = \eta_2 = 2/3$ in (12) and (13), we took

$$\ell_1 = 1.087, \qquad \ell_2 = 0.721. \tag{37}$$

These values satisfy the conditions (21) and (24) with $\xi_2 = 67.7\%$ and $\xi_1 = 71.4\%$, respectively.

Note that in order to confirm the role of the key values of $|T_{v_2v_1}(0)|$ and $|T_{v_1v_2}(0)|$ in the limiting function themselves, we did not completely perform the optimization in (29) to obtain the controller (33), which has only an acceptable servo performance.

(iv) Simulation conditions:

(a) Sensor failure: Sensor 1 fails at $t = 60$ as $\hat{y}_{10} = 0.1$. That is, the measured value after the failure is given by $\hat{y}_1(t) = 0.1 + n_1(t)$ $(t > 60)$, where $n_1(t)$ is a white Gaussian noise given in (d) below.

(b) Reference signals:

$$r_1(t) = \begin{cases} 0, & 0 \le t < 20 \\ 1, & 20 \le t \end{cases} \tag{38}$$

$$r_2(t) = \begin{cases} 0, & 0 \le t < 40 \\ 0.5, & 40 \le t < 80 \\ 1, & 80 \le t, \end{cases} \tag{39}$$

where $r_2(t)$ into a normal loop is changed at $t = 80$ after the sensor failure at $t = 60$.

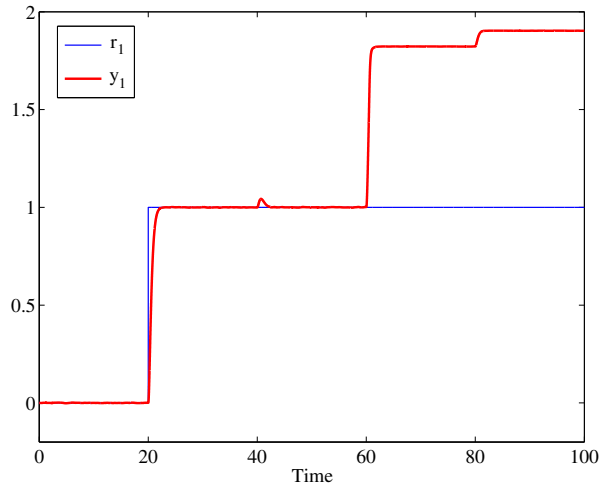

Fig. 4. Response in y_1.

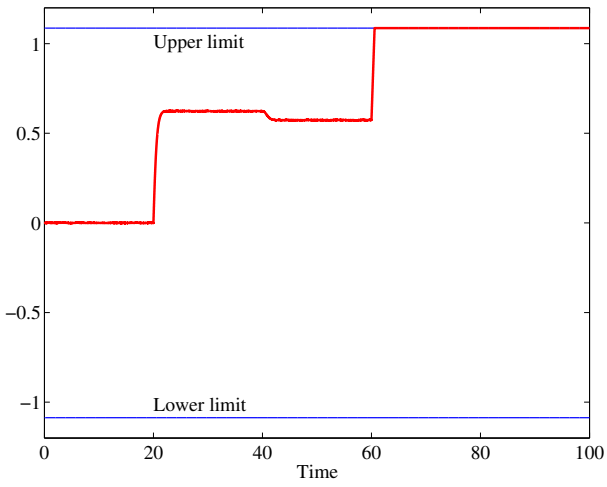

Fig. 6. Response in v_1.

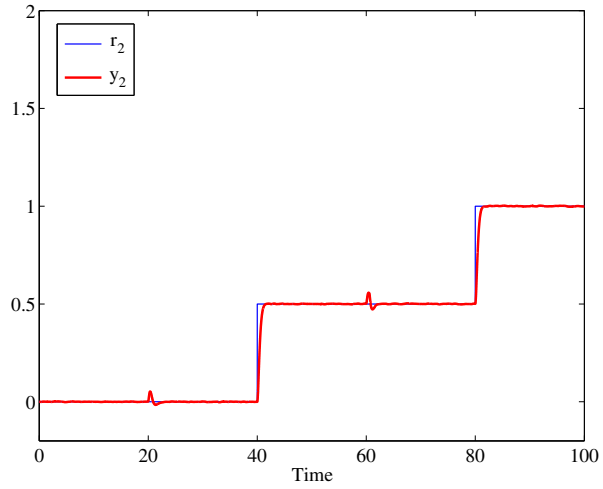

Fig. 5. Response in y_2.

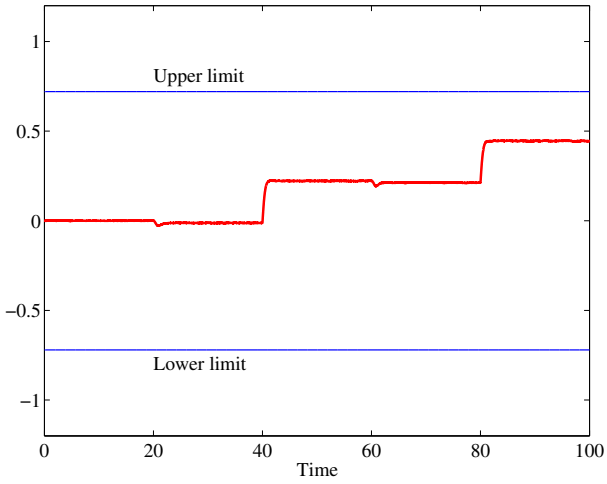

Fig. 7. Response in v_2.

(c) Model error: We suppose that each element of P in (30) includes a maximum error of 3% whose concrete value was determined by the uniform distribution. The actual plant used in the simulation was as follows:

$$\left[\begin{array}{cccc|cc} -4.073 & -2.046 & -2.057 & 1.947 & 1.001 & 0 \\ 2.009 & -3.887 & -1.013 & 2.022 & 0 & -0.979 \\ 0.981 & -2.998 & -4.000 & 2.918 & 1.019 & 1.010 \\ 1.969 & 0 & -0.998 & -1.949 & -2.038 & 1.001 \\ \hline 1.028 & 2.036 & -0.996 & 0 & 0 & 0 \\ 1.009 & -0.997 & 1.020 & 0.978 & 0 & 0 \end{array}\right]. \tag{40}$$

(d) Sensor noises: n_1 and n_2 are white Gaussian noises generated by the normal distribution $N(0, 0.03^2)$, where they are saturated by the limits ± 0.1. That is, the measured value by normally-functioning Sensor i $(i = 1, 2)$ is $\hat{y}_i(t) = y_i(t) + n_i(t)$, where $y_i(t)$ is the measured output of the plant.

(v) Simulation result: Figures 4 and 5 show the responses in the measured outputs y_1 and y_2 with the reference signals r_1 and r_2, respectively. Figures 6 and 7 show the responses in the outputs v_1 and v_2 of the limited integrators with the limits $\pm \ell_1$ and $\pm \ell_2$, respectively.

The responses in y_1 and y_2 immediately after $t = 20$ and $t = 40$ shows that the servo performance in the normal case is satisfactory.

Immediately after Sensor 1 fails at $t = 60$, a ramp signal appears in v_1 on the failed Loop 1. Although a ramp signal appears also in v_2 on the normal Loop 2, its gradient is sufficiently smaller than that of v_1 in accordance with (16).

Thus, v_1 approaches the upper limit at a sufficiently faster speed than v_2. Then, it reaches the upper limit ℓ_1 sufficiently early. On the other hand, v_2 does not reaches the upper limit ℓ_2, and converges to a value between the limits in accordance with (21). Although y_1 on the failed Loop 1 converges to a value away from r_1, the effect on a constant disturbance v_1 to y_2 is eliminated by the servo performance of the normal Loop 2.

The servo performance of the normal Loop 2 can satisfactorily respond to the change in r_2 at $t = 80$. Here, v_1 is hold at the upper limit ℓ_1 by the limiting function, while v_2 converges to a value between the limits in accordance with (21).

V. Conclusions

In this paper, we obtained the key for the limiting function implemented in limited integrators to behave effectively as the measure against ramp signals caused by sensor failures for the first time. Then, the limiting function and a controller can be designed in a unified framework of simultaneous optimization with consideration given to the servo performance in the normal case and in faulty cases. The obtained result succeeds in establishing the potential applicability of limited integrators to fault-tolerant servo systems.

We have already obtained the result on fault-tolerant servo systems using limited integrators with variable limits for better performance immediately after sensor failures.

An important future work is to extend the result obtained in this paper to robust servo systems. It is important to clarify the relationship between the robust servo performance and the limiting function.

Acknowledgment

This research was supported by Grant #22560440, Grant-in-Aid for Scientific Research (C), Ministry of Education, Culture, Sports, Science and Technology, Japan.

References

[1] E.J. Davison, "The robust control of a servomechanism problem for linear time-invariant multivariable systems," *IEEE Transactions on Automatic Control*, Vol.21, No.1, pp.25–34. 1976.

[2] International Electrotechnical Commission (IEC), *IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems*, 2nd edition, Geneva, 2010.

[3] A.N. Gündeş, "Stability of feedback systems with sensor or actuator failures: Analysis," *International Journal of Control*, Vol.56, No.4, pp.735–753, 1992.

[4] R.J. Veillette, J.V. Medanic, and W.R. Perkins, "Design of reliable control systems," *IEEE Transactions on Automatic Control*, Vol.37, No.3, pp.290–304, 1992.

[5] C.-J. Seo and B.K. Kim, "Robust and reliable H_∞ control for liner systems with parameter uncertainty and actuator failure," *Automatica*, Vol.32, No.3, pp.465–467, 1996.

[6] J. Stoustrup and V.D. Blondel, "Fault tolerant control: A simultaneous stabilization result," *IEEE Transactions on Automatic Control*, Vol.49, No.2, pp.305–310, 2004.

[7] K. Suyama and N. Sebe, "Probabilistic safety management of control laws against deviations from normal operating-range," in *Proceedings of the Conference on Control and Fault-Tolerant Systems*, Nice, October 2010, pp.442–449.

[8] N. Sebe and K. Suyama, "Fault-tolerant servo systems against actuator failures," in *Preprints of the 7th IFAC Symposium on Robust Control Design*, Aalborg, June 2012, pp.499–504.

[9] A.N. Mete and A.N. Gündeş, "MIMO controller synthesis with integral-action integrity," *Automatica*, Vol.44, No.1, pp.128–134, 2008.

[10] N. Sebe, "A new dilated LMI characterization and iterative control system synthesis," in *Proceedings of the 11th IFAC/IFORS/IMACS/IFIP Symposium on Large Scale Systems: Theory and Applications*, Gdańsk, July 2007, 6 pages.