Available online at www.sciencedirect.com

ScienceDirect

IFAC PapersOnLine 50-1 (2017) 10369–10376

Support technology for safe preventive maintenance of control systems

Koichi Suyama * **Noboru Sebe** **

* *Tokyo University of Marine Science and Technology Etchujima, Koto-ku, Tokyo 135-8533, Japan (e-mail: suyama@kaiyodai.ac.jp).*
** *Kyushu Institute of Technology Kawazu, Iizuka, Fukuoka 820-8502, Japan (e-mail: sebe@ai.kyutech.ac.jp).*

Abstract: On the basis of fault-tolerant control theory and switching $\mathcal{L}_2$ gain analysis, we propose a new maintenance support technology to implement an operating state suitable for safely performing preventive maintenance of each subsystem, where the safety of the bidirectional transitions between normal operation and an operating state is guaranteed.

Keywords: Maintenance; Control systems; Corrective actions; Fault tolerance; Reset.

1. INTRODUCTION

Fault-tolerant control theory has been studied mainly on the basis of measures after control systems fall out of normal operation due to hardware failures. For example, several studies on controller design have been conducted to achieve tolerance against failures in actuators and/or sensors without their detection/isolation (e.g., Veillette, Medanic, and Perkins (1992), Stoustrup and Blondel (2004), Mete and Gündeş (2008)). Fault-tolerant control theory certainly improves the availability performance of control systems. However, for further improving the availability performance, preventive maintenance is also important. In addition, product liability makes it obligatory for manufacturers to present appropriate and effective procedures of preventive maintenance for each product.

However, there are many control systems on which it is difficult to safely perform preventive maintenance. For example, especially in the process industry, "maintenance-free technology" has been studied because preventive maintenance of manufacturing plants under safe conditions or operating states is difficult. The international standards on maintenance (e.g., IEC 60300-3-11 (2009)) and the well-known references in the field of safety engineering (e.g., Kumamoto (2010)) only explain required work items of preventive maintenance, such as component replacement. There are no systematic studies on an operating state suitable for safely performing preventive maintenance.

In this paper, we propose a new maintenance support technology to
(a) achieve an operating state suitable for safely performing preventive maintenance of each subsystem
(b) under guaranteed safety of the bidirectional transitions between normal operation and the operating state.

The proposed technology is based on the above-mentioned fault-tolerant controller design and switching $\mathcal{L}_2$ gain analysis, such as that described in Suyama and Sebe (2015). Although it has been stated that online maintenance can be performed in control systems by designing the controller appropriately, no concrete procedures for maintenance have been presented up to now. One reason is that even in such designed control systems, protection against the fluctuation caused by the bidirectional transitions between normal operation and an operating state where maintenance is performed is difficult to evaluate and guarantee. In the proposed technology, by using the switching $\mathcal{L}_2$ gain to evaluate the magnitude and severity of the fluctuation in transient responses after a switch (Suyama and Sebe, 2015), the safety of the bidirectional transitions is evaluated and guaranteed.

The proposed maintenance support technology, which for the first time focuses on an operating state suitable for preventive maintenance, is useful for improving not only the maintainability performance directly but also the availability performance of control systems indirectly. The discussion in this paper clarifies that we can establish an appropriate and effective procedure for preventive maintenance of control systems in the controller design step.

The following notations are used in this paper. $T_{zw}(s)$: the transfer function matrix from a signal w to another z, and $\|G\|_\infty$: the $\mathcal{H}_\infty$ norm of a transfer function matrix G. $\mathcal{L}_{2\,(a,b)} = \left\{ x(t) \,\middle|\, \|x(t)\|_{2\,(a,b)} < \infty \right\}$, where $\|x(t)\|_{2\,(a,b)}$ denotes the the $\mathcal{L}_2$ norm defined by $\|x(t)\|_{2\,(a,b)} = \left[\int_a^b x^{\mathrm{T}}(t)x(t)dt \right]^{\frac{1}{2}}$.

2. SWITCHING $\mathcal{L}_2$ GAIN

2.1 Switch to be analyzed

Suppose that a linear time-invariant (LTI) system H_p switches to another LTI system H_f with a state transition at the switching time $t = t_0$.

Suppose that the system before the switch (i.e., the pre-switch system) is represented by

Peer review under responsibility of International Federation of Automatic Control.
10.1016/j.ifacol.2017.08.1690

$$H_p\colon \begin{cases} \dot{x}_p(t) = A_p x_p(t) + B_p w(t) \\ z(t) = C_p x_p(t) + D_p w(t), \end{cases} \quad t \le t_0, \tag{1}$$

where $x_p(t) \in \mathbb{R}^{n_p}$ $(t \le t_0)$ is the internal state, $w(t) \in \mathbb{R}^{n_i}$ is the input, and $z(t) \in \mathbb{R}^{n_o}$ is the output. We assume that A_p is stable, (A_p, B_p) is controllable, and (C_p, A_p) is observable.

Suppose that the system after the switch (i.e., the post-switch system) is represented by

$$H_f\colon \begin{cases} \dot{x}_f(t) = A_f x_f(t) + B_f w(t) \\ z(t) = C_f x_f(t) + D_f w(t), \end{cases} \quad t > t_0, \tag{2}$$

where $x_f(t) \in \mathbb{R}^{n_f}$ $(t > t_0)$ is the internal state and $w(t)$, $z(t)$ are the same input and output as in the pre-switch system H_p. We assume that A_f is stable, (A_f, B_f) is controllable, and (C_f, A_f) is observable.

Suppose that the following internal state transition occurs around the switch:

$$x_f(t_{0+}) = S x_p(t_0), \tag{3}$$

where $S \in \mathbb{R}^{n_f \times n_p}$ is a constant matrix. Using the matrix S, we represent controller resets and/or additions possibly accompanying the restart (Suyama and Sebe, 2015).

2.2 Switching $\mathcal{L}_2$ gain

Suyama and Sebe (2015) proposed the following switching $\mathcal{L}_2$ gain based on responses on the post-switch side alone:

$$\hat{\gamma} = \sup_{w(t) \in \mathcal{L}_2(-\infty,\infty)\setminus\{0\}} \frac{\|z(t)\|_{2\,(t_0,\infty)}}{\|w(t)\|_{2\,(-\infty,\infty)}}. \tag{4}$$

This switching $\mathcal{L}_2$ gain evaluates the magnitude and severity of the fluctuation in transient responses after a switch.

By using the following theorem, we obtain the value of $\hat{\gamma}$:

Theorem 1. (Suyama and Sebe, 2015) For a given $\gamma > 0$, the switching $\mathcal{L}_2$ gain $\hat{\gamma}$ satisfies $\hat{\gamma} < \gamma$ if and only if there exist $\tilde{X}_p \succ O$ and $\tilde{X}_f \succ O$ satisfying the following LMIs:

$$\begin{bmatrix} \tilde{X}_p A_p + A_p^{\mathrm{T}} \tilde{X}_p & \tilde{X}_p B_p \\ B_p^{\mathrm{T}} \tilde{X}_p & -\gamma I \end{bmatrix} \prec O \tag{5}$$

$$\begin{bmatrix} \tilde{X}_f A_f + A_f^{\mathrm{T}} \tilde{X}_f & \tilde{X}_f B_f & C_f^{\mathrm{T}} \\ B_f^{\mathrm{T}} \tilde{X}_f & -\gamma I & D_f^{\mathrm{T}} \\ C_f & D_f & -\gamma I \end{bmatrix} \prec O \tag{6}$$

$$\tilde{X}_p - S^{\mathrm{T}} \tilde{X}_f S \succ O. \tag{7}$$

This theorem also implies that the switching time t_0 does not affect the value of $\hat{\gamma}$.

3. A FRAMEWORK FOR SAFE PREVENTIVE MAINTENANCE

Suppose that preventive maintenance of a control system is performed for each subsystem S_i $(i = 1, 2, 3 \ldots)$. The framework for safe preventive maintenance of Subsystem S_i that the proposed maintenance support technology presents is shown in Fig. 1. State i is the operating state where S_i is stopped for its maintenance ("gray-colored" S_i indicates its stoppage); State $i\,\mathrm{m}$ is the operating state that is suitable for safely performing its maintenance. Transition i, j $(j = 1, 2, 3, 4)$ denotes a system transition between two operating states.

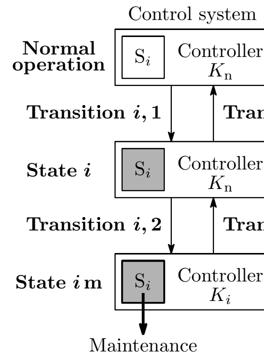

Fig. 1. Proposed framework for preventive maintenance.

3.1 Normal operation

In general, a control system should achieve superlative performance in normal operation among several operating states. That is, Controller K_{n} used in normal operation should be designed so that it can achieve optimal performance under other requirements, such as tolerance against a stoppage of a subsystem for its maintenance.

3.2 Stoppage of a subsystem for maintenance

The stoppage of Subsystem S_i is necessary for preventive maintenance. It leads the control system from normal operation to State i in Fig. 1. This is Transition i,1.

Note that the control system — except S_i — continues to operate. The stability and acceptable performance of the operating part in State i are guaranteed by the tolerance against the stoppage of S_i that is predesigned in Controller K_{n}. We thus design Controller K_{n} using fault-tolerant control theory. In general, owing to the stoppage of S_i, the performance is lower than that in normal operation.

Furthermore, the safety of Transition i,1 should be also guaranteed by tolerance against the stoppage of S_i. The fluctuation in the transient responses after Transition i,1 should be well suppressed so that deviation from normal operating range does not occur. The magnitude and severity of the fluctuation after Transition i,1 can be evaluated by the value of $\hat{\gamma}_{i,1}$, the switching $\mathcal{L}_2$ gain $\hat{\gamma}$ for Transition i,1. A smaller $\hat{\gamma}_{i,1}$ implies that the fluctuation is suppressed in a more effective manner; then, Transition i,1 can be performed more safely. Thus, Controller K_{n} should be predesigned so that the value of $\hat{\gamma}_{i,1}$ is smaller than an acceptable level.

Remark 1. If Controller K_{n} such that $\hat{\gamma}_{i,1}$ is smaller than an acceptable level does not exist, then we consider the following countermeasures for guaranteeing the safety of Transition i,1.

- We stop Subsystem S_i after leading the control system to an operating state that is suitable for the stoppage, as in Asai (2005).
- From $\hat{\gamma}_{i,1}$ and an acceptable level, we have the permission condition for Transition i,1, as in Suyama and Kosugi (2013). Only when the internal state of the control system satisfies the condition, we stop Subsystem S_i.

The same considerations apply to Transitions i,2, i,3, and i,4.