Realization of safety function against deviations from normal operating-range in control laws

Koichi Suyama* Nobuko Kosugi**

* Tokyo University of Marine Science and Technology
Etchujima, Koto-ku, Tokyo 135-8533, Japan
(e-mail: suyama@kaiyodai.ac.jp).
** Tokyo University of Marine Science and Technology
Etchujima, Koto-ku, Tokyo 135-8533, Japan
(e-mail: kosugi@kaiyodai.ac.jp).

Abstract: This paper proposes safety function in control laws to reduce the frequency of events that a physical value in a control system deviates from its normal operating-range. This safety function is realized mainly by the safety ability to suppress the fluctuations of transient responses after a device failure in order to prevent the deviations from the normal operating-range on the basis of dependability function to maintain the stability and the control performance even if the system is not in the normal operation. The proposed safety function in control laws can supplement ordinary safety-related systems in risk reduction according to international safety standards such as IEC 61508, where its contribution can be evaluated quantitatively.

Keywords: Fault-tolerant systems; Safety; Control laws; Dependability; Transient deviation.

1. INTRODUCTION

As clearly defined in many international standards such as IEC60050 [1990] and IEC61508 [2010], safety and dependability are completely different in content (see Fig. 1). Dependability is the idea on the maintenance of designed system performance. Hence, dependability function is the ability to maintain the stability and the control performance of the control system even if the system is not in the normal operation, i.e., the measures against abnormal “states.” On the other hand, safety is evaluated by risk, which is combination of the probability of occurrence of harmful events and their severity. Hence, safety function can be evaluated in the ability to reduce harmful event frequency, i.e., the measures against “events.”

In the ordinary safety measures, if a safety-related system implemented outside detects that a physical value deviates from its normal operating-range, then it performs its design function to prevent harmful events as far as possible. Hence, of course, it is desirable to reduce the frequency of the deviations from the normal operating-range from a viewpoint of risk reduction required in international standards on safety such as IEC 61508.

The authors have proposed the ability realized in control laws for maintaining the stability and the control performance not only in the normal operation but also under fault conditions (Suyama [2008]). Strictly speaking, this is dependability function. In fault-tolerant control system design, safety function to reduce the frequency of the deviations from the normal operating-range is required.

However, such safety function is difficult to realize, because it is also required to suppress the fluctuations of transient responses immediately after a failure.

A number of studies have been made on the issue of suppressing abrupt or “bumpy” responses by using “bumpless transfer” (Turner [2000]) and other concepts. For example, in Asai [2002] and Asai [2005], the $L_2$ gain analysis using a Hankel-like operator is proposed to evaluate the effects of switchings quantitatively. However the existing studies mainly consider switchings of the controllers and they assume that the switching time is known a priori for activating an additional controller. They can not be applied to fault-tolerant control systems, where the time when the failure occurs is usually unpredictable.

This paper proposes safety function in control laws to reduce the frequency of events that a physical value in a control system deviates from its normal operating-range. The safety function is realized

---

1 The first author is an official member of IEC TC56: Dependability and Technical Resource of Maintenance team for IEC 61508.
• mainly by the safety ability to suppress the fluctuations of transient responses after a device failure in order to prevent the deviations from the normal operating-range
• on the basis of dependability function (Suyama [2008]) to maintain the stability and the control performance of the control system even if the system is not in the normal operation.

The realization framework clarifies the possibility that the safety function in control laws can supplement ordinary safety-related systems in risk reduction according to international safety standards such as IEC 61508, where its contribution can be evaluated quantitatively.

2. SAFETY FUNCTION IN CONTROL LAWS

2.1 IEC 61508

Figure 2 illustrates the overall system configuration considered in IEC 61508. A control system consists of an equipment under control (EUC), i.e., a controlled object, and a basic control system (BCS) which operates EUC in the desired manner. IEC 61508 requests to reduce the initial risk in EUC and BCS by safety measures so that the residual risk of the overall system is less than the predetermined tolerable risk level.

A SRS has safety function to achieve or to maintain a safe state of the EUC. Because a hardware failure occurs at a random time in a safety-related system (SRS), there is the possibility that the SRS cannot perform its safety function. IEC 61508 assesses functional safety of an electrical/electronic/programmable electronic (E/E/PE) SRS, ability to perform its safety function, using four safety integrity levels (SILs) for two kinds of operation modes, low demand / continuous mode. If a SRS shoulders a heavy burden for risk reduction, it is required to fit a higher SIL.

Table 1. Safety integrity levels in low demand mode of operation.

<table>
<thead>
<tr>
<th>SIL</th>
<th>Average probability of failure to perform its design function on demand (PFD&lt;sub&gt;avg&lt;/sub&gt;)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>$\geq 10^{-5}$ to $&lt; 10^{-4}$</td>
</tr>
<tr>
<td>3</td>
<td>$\geq 10^{-4}$ to $&lt; 10^{-3}$</td>
</tr>
<tr>
<td>2</td>
<td>$\geq 10^{-3}$ to $&lt; 10^{-2}$</td>
</tr>
<tr>
<td>1</td>
<td>$\geq 10^{-2}$ to $&lt; 10^{-1}$</td>
</tr>
</tbody>
</table>

2.2 Initial events

Consider a control system shown in Fig. 2. Let Devices 1,..., N denote Sensors 1,..., N<sub>s</sub> and Actuators 1,..., N<sub>a</sub>, where $N = N_s + N_a$.

A single failure, a functional stoppage, probabilistically occurs in Device k in accordance with the exponential distribution with the occurrence rate, single failure rate, $\lambda_k, k = 1,\ldots,N$.

Repair time of a failed Device k probabilistically follows the exponential distribution with the mean time to repair, MTTR<sub>k</sub>, $k = 1,\ldots,N$. The repair rate of Device k is given by $\mu_k = 1/\text{MTTR}_k$. This is an ordinary formulation in the field of safety/reliability engineering.

We assume the followings.

Assumption 1. The failure rates of the logic solver and the EUC are sufficiently smaller than $\lambda_k$, and their effect is negligible.

Assumption 2. A demand on such safety measures as an E/E/PE SRS occurs when a physical value in the control system deviates from its normal operating-range.

Assumption 3. The frequency of the deviations from the normal operating-range by control device failures is sufficiently higher than the frequency by other causes.

Note that the deviations from the normal operating-range are caused not only by the system instability but also by the fluctuations of transient responses after a failure.

2.3 Device context

Device k ($k = 1,2,\ldots,N$) is in either of the normal operation or a fault as described in the following:

$$\delta_k = \begin{cases} 0, & \text{Device k : normal} \\ 1, & \text{Device k : fault} \end{cases} \quad (k = 1,2,\ldots,N). \quad (1)$$

Describe a device situation of the control system by $(\delta_1,\delta_2,\ldots,\delta_N)$, which is referred to hereafter as a “device context” except $(0,\ldots,0)$: the normal operation, “Normal.” For example, $(1,0,0,0,\ldots,0)$ represents a device situation where only Device 1 is in a fault, and $(0,1,1,0,\ldots,0)$ represents a device situation where only Devices 2 and 3 are in a fault. Possible device contexts are $2^N - 1$ in all.

2.4 Safety function in control laws

Safety function against the deviations from the normal operating-range is realized on the basis of dependability

$^2$ In IEC 61508 repair process is quantitatively treated by MTTR.
function to maintain the stability and the control performance of the control system even if the system is not in the normal operation. This dependability function can be identified with a set of device contexts, S, where the control system with the control law is stable.

The additional safety ability to suppress the fluctuations of transient responses immediately after a failure is for preventing the deviations from the normal operating-range of transient responses immediately after a failure is for (3) the controlled object is assumed to be strictly proper for simplicity, however, the discussion can easily be extended to the case where where $y(t) = C_G x_G(t) + D_{G21} w(t) + D_{G22} u(t)$. Suppose that a control law is given by

$$K : \begin{cases} \frac{dx_K(t)}{dt} = A_K x_K(t) + B_K y(t) \\ u(t) = C_K x_K(t) + D_K y(t) \end{cases} \quad (4)$$

where $x_K(t)$ is the internal state of the control function.

The transfer function matrix of the closed-loop control system from $w(t)$ to $z(t)$ in the normal operation is obtained by $F_l(G_{org}, K)$ where $F_l$ denotes lower LFT (see Fig. 3), and the normal-case control performance is evaluated by

$$\gamma_0 = \| F_l(G_{org}, K) \|_{\infty} \quad (5)$$

where $\| \cdot \|_{\infty}$ denotes $\mathcal{H}_\infty$ norm. The control system in the normal operation $F_l(G_{org}, K)$ is concretely described by

$$F_l(G_{org}, K) : \begin{cases} \frac{dx(t)}{dt} = A_0 x(t) + B_0 w(t) \\ z(t) = C_0 x(t) + D_0 w(t) \end{cases} \quad (6)$$

where $x(t) = [x_G(t), x_K(t)]^T \in \mathbb{R}^n$ is the internal state of the control system.

By a failure in a device, i.e., by a switching in the generalized plant including the device, the transfer function matrix of the closed-loop control system from $w(t)$ to $z(t)$, which is obtained by the above in Normal, is switched from one to another. Considering that the fluctuations of transient responses caused by such a switching can be evaluated by the switching $L_2$ gain [Hespanha [2003], Sebe [2010]], we formulate the deviations from the normal operating-range using the $L_2$ norm of a physical value as follows.

Consider the $L_2$ norm of a signal vector $f(t)$ defined by

$$\| f(t) \|_2 = \left( \int_{-\infty}^{\infty} f^T(t) f(t) dt \right)^{\frac{1}{2}} \quad (7)$$

which corresponds to the total energy of the signal. In this paper the deviations from the normal operating-range are formulated by the following two assumptions.

**Assumption 4.** The exogenous input $w(t)$ satisfies

$$\| w(t) \|_2 \leq \overline{\gamma} (= \text{constant}) \quad (8)$$

**Assumption 5.** If the evaluated output $z(t)$ satisfies

$$\| z(t) \|_2 \leq \overline{\gamma} (= \text{constant}) \quad (9)$$

the deviations from the normal operating-range do not occur.

**Remark 1.** Suppose that the normal operating-range for each evaluated output $z_i(t)$ of $z(t) = [z_1(t), z_2(t), \ldots, z_p(t)]^T = [-\alpha_i, \alpha_i]$ ($\alpha_i > 0$). The $\overline{\gamma}$ in Assumption 5 can conservatively be set by
where $T_0 (>0)$ is a sufficiently short interval. This is the limiting value, even if all the energy of $z(t)$ is concentrated to $z_i(t)$ ($i \in (0, T_0)$), which has the narrowest normal operating-range, pulsed fluctuations of its transient response do not cause the deviations from the range. The $T_0$ is determined in consideration of the worst transient responses in some switchings, which should be obtained beforehand. A smaller value of $T_0$ results in a smaller value of $\tau$, which gives a more conservative assessment result because the possibility of the deviations caused by smaller energy is taken into consideration.

3. REPRESENTATIVE SAFETY FUNCTIONS

In the case of a control system with $N$ Devices, there are $2^N - 1$ device contexts, and there are a enormous number, $2^{2N-1} - 1$, of possible safety functions, i.e., possibilities of the set $S$. Hence we introduce an idea of representative safety functions. It plays an essential role in the proposed realization framework for the following reasons.

- All representative safety functions can be expressed in the simple and fixed-length structure.
- They can be enumerated systematically.
- A representative safety function includes no isolated device contexts.
- The set of all possible switching considered for a representative safety function can easily be obtained.

3.1 Definition and expression

Device Group In order to consider a representative safety function in control laws, define $m$-th $n$-DG (device group), $G_{(n,m)} = \{Device \; k_{n,m,1}, \; Device \; k_{n,m,2}, \; \ldots, \; Device \; k_{n,m,n}\}$, where $n$ denotes the number of devices in the DG, and $m$ denotes the order in $n$-DGs (in the expression of a representative safety function). Let $S_{(n,m)}$ denote the set of $2^n - 1$ device contexts, except Normal: $(0, 0, \ldots, 0)$, all possible normal/fault combinations of the devices in $G_{(n,m)}$.

Representative safety function Consider a representative safety function by

$$\{G_{(n,m)} \; (m, n = 1, 2, 3, \ldots) | G_{(n,m_1)} \cap G_{(n,m_2)} = \phi ((n_1, m_1) \neq (n_2, m_2))\}.$$ (11)

It can be identified with the set of device contexts

$$S = \bigcup_{n,m} S_{(n,m)}.$$ (12)

Define $G_{rest} = \{Device \; 1, \ldots, \; Device \; N\} \setminus (\bigcup_{n,m} G_{(n,m)})$.

Note that each device context in a representative safety function is reachable from Normal by sequences of single failures through only other device contexts in the representative safety function. That is, a representative safety function includes no “isolated” device contexts.

In this paper such a representative safety function is expressed by $[y_1, y_2, \ldots, y_N]$ where

$$i_k = \begin{cases} 1 & Device \; k \in 1-DG \; \text{Device} \; k \in m-th \; n(\geq 2)-DG \; \text{Device} \; k \in G_{rest} \end{cases}$$

If $i_k = i_{k_1}$, Devices $k_1$ and $k_2$ belong to the same device group. $n(\geq 2)$-DGs including $n$ devices are expressed by $n, n/2, n/3, n/4, \ldots$, in the order of appearance in order of device numbers. This simple and fixed-length expression can make it possible to enumerate all representative safety functions easily and systematically.

Possible switching For an $m$-th $n$-DG $D_{G(n,m)}$, consider a transition from a device context $(\delta'_1, \delta'_2, \ldots, \delta'_N) \in (Normal \cup S_{(n,m)})$ to $(\delta_1, \delta_2, \ldots, \delta_N) \in S_{(n,m)}$ caused by a failure in Device $k$, where $\delta_k = 1$ and

$$\delta'_k = \begin{cases} 0 & (k' = k) \\ \delta_k' & (k' \neq k) \end{cases}.$$ (13)

Denote such a “switching” by $((\delta'_1, \delta'_2, \ldots, \delta'_N), (\delta_1, \delta_2, \ldots, \delta_N))$. If a before-switching context $(\delta'_1, \delta'_2, \ldots, \delta'_N)$ is Normal, it can be written so.

Let $\Theta_{(n,m)}$ denote the set of all $n \cdot 2^{n-1}$ possible switchings considered for $D_{G(n,m)}$, and obtain the set of all possible switchings

$$\Theta = \bigcup_{n,m} \Theta_{(n,m)}.$$ (14)

Example A representative safety function $[0, 2, 2, 2/2, 2/2, 2/2, 2/2]$ including 3 DGs maintains the stability of the control system in the following 7 device contexts. In the proposed realization framework, the safety measures are taken against the deviations from the normal operating-range at the following 9 possible switchings by control law design.

(i) For 1st 1-DG, $D_{G(1,1)} = \{Device \; 5\}$

$S_{(1,1)} = \{0, 0, 0, 0, 0, 0\}$

$\Theta_{(1,1)}$ includes one switching

- from Normal to $\{0, 0, 0, 0, 0, 1\}$ by failure in Device 5.

(ii) For 1st 2-DG, $D_{G(2,1)} = \{Device \; 2, \; Device \; 6\}$

$S_{(2,1)} = \{0, 0, 0, 0, 0, 0\}$

$\Theta_{(2,1)}$ includes the following four switchings:

- from Normal to $\{0, 0, 0, 0, 0, 1\}$ by a failure in Device 2
- from Normal to $\{0, 0, 0, 0, 0, 1\}$ by a failure in Device 6
- from $\{0, 1, 0, 0, 0, 0\}$ to $\{0, 1, 0, 0, 0, 1\}$ by a failure in Device 6
- from $\{0, 0, 0, 0, 0, 1\}$ to $\{0, 1, 0, 0, 1, 0\}$ by a failure in Device 2.

(iii) For 2nd 2-DG, $D_{G(2,2)} = \{Device \; 3, \; Device \; 4\}$

$S_{(2,2)} = \{0, 0, 0, 0, 0, 0\}$

$\Theta_{(2,2)}$ includes the following four switchings:

- from Normal to $\{0, 0, 0, 0, 0, 0\}$ by a failure in Device 3
- from Normal to $\{0, 0, 0, 0, 0, 0\}$ by a failure in Device 4
- from $\{0, 0, 1, 0, 0, 0\}$ to $\{0, 1, 1, 0, 0\}$ by a failure in Device 4
- from $\{0, 0, 0, 1, 0, 0\}$ to $\{0, 0, 1, 1, 0, 0\}$ by a failure in Device 3.

3.2 Class

In order to enumerate all representative safety functions, introduce a class of them $<j_1, j_2, \ldots, j_N>$. $J_n (n = 2, 3, \ldots)$ denotes the number of $n$-DGs, and

$$j_1 = \begin{cases} 1, & \text{a 1-DG and/or a device } \in G_{rest} \text{ exists} \\ 0, & \text{otherwise} \end{cases}$$

For example, in the case where $N = 6$, a representative safety function $[0, 2, 2, 2/2, 2/2, 2/2, 2/2]$ includes two 2-DGs and an 1-DG, and belongs to the class $<1, 2, 0, 0, 0, 0>$.
4. REALIZATION FRAMEWORK

The inputs of the proposed framework for realizing safety function in control laws against the deviations from the normal operating-range are itemized as follows:

- generalized plant $G_{\text{org}}$
- failure rates and MTTRs of the devices
- $\varpi$ in Assumption 4
- $\varpi$ in Assumption 5
- demand target frequency $DF_{\text{tar}}$.

Remark 2. For a given target hazardous event frequency $HEF_{\text{tar}}$, the average probability of a failure to perform its design function on demand $PFD_{\text{avg}}$ of an E/E/PE SRS should be

$$PFD_{\text{avg}} \leq \frac{HEF_{\text{tar}}}{DF_{\text{tar}}}.$$  (15)

Then, a target safety integrity level, SIL_{\text{tar}}, is determined by Table 1. We should install an E/E/PE SRS of SIL_{\text{tar}}. Hence, taking $HEF_{\text{tar}}$ and SIL_{\text{tar}} into consideration, we should set a value of target demand frequency $DF_{\text{tar}}$.

The output of the proposed framework is a control law with the optimal normal-case control performance subject to the safety requirement that $DF < DF_{\text{tar}}$.

4.1 Step 1: threshold for switching $L_2$ gain

From $\varpi$ in Assumption 4 and $\varpi$ in Assumption 5, define the threshold for switching $L_2$ gain by

$$\overline{\varrho} = \overline{\varpi}.$$  (16)

Note that the deviations from the normal operating-range do not occur by the fluctuations of transient responses at the system switching of switching $L_2$ gain value less than or equal to $\overline{\varrho}$ regardless of the internal state of the control system at the switching and the exogenous input $u(t)$ after the switching. Conversely, there is the possibility that the deviations occur at the system switchings of switching $L_2$ gain value larger than $\overline{\varrho}$.

4.2 Step 2: all representative safety functions satisfying dependability requirement

Step 2-1: all representative safety functions For each class of representative safety functions, enumerate all representative safety functions, by using selection of $n$ figures $\cdot 1 - (1/2)^{m-1}$ out of device numbers $1, 2, \ldots, N$ for $m$-th $n$-DG and binary digit.

For example, in the case where $N = 6$, the class $< 1, 0, 0, 0, 0 >$ includes $2^6 - 1 = 63$ safety functions: $[1, 0, 0, 0, 0], [0, 1, 0, 0, 0], [1, 1, 0, 0, 0], [0, 0, 1, 0, 0], \ldots, [1, 1, 1, 1, 1, 1]$, and the class $< 1, 0, 0, 1, 0, 0 >$ includes $[4, 4, 4, 4, 0, 0], [4, 4, 4, 4, 1, 0], [4, 4, 4, 4, 1, 1], [4, 4, 0, 0, 0], [4, 4, 4, 1, 0], [4, 4, 4, 1, 1], [4, 4, 4, 1, 1], [4, 4, 4, 0, 0], [4, 4, 4, 0, 1], [4, 4, 4, 1, 1], [4, 4, 4, 1, 1], [4, 4, 4, 1, 1], [4, 4, 4, 0, 1], [4, 4, 4, 1, 1], and so on.

Step 2-2: frequency of deviations caused by system destabilization For each representative safety function $[i_1, i_2, \ldots, i_N]$, obtain the frequency of the deviations caused by the system destabilization $\omega_{\text{unstable}}([i_1, i_2, \ldots, i_N])$ by Markov analysis as follows.

Suppose that a representative safety function $[i_1, i_2, \ldots, i_N]$ can be identified with the set of device contexts $S = \{S_1, S_2, \ldots, S_{N_{DC}}\}$ where $N_{DC}$ denotes the number of them. On the state transition diagram, the control system transits between $N_{DC} + 2$ states, $S_0$ (Normal), $S_1$, $S_2$, $S_{N_{DC}}$, $S_{N_{DC} + 1}$, by failures or repairs in control devices, where we denote all device contexts which do not belong to $S$ by $S_{N_{DC} + 1}$ on the diagram. If the system transits into $S_{N_{DC} + 1}$ on the diagram, it falls into an unstable state.

Define $p(t) = [p_0(t) \ p_1(t) \ \cdots \ p_{N_{DC}}(t) \ p_{N_{DC} + 1}(t)]^T$, where $p_i(t)$ denotes the probability that the system is in $S_i$ at $t$. Then obtain the Markov differential equation

$$\frac{dp(t)}{dt} = Qp(t)$$  (17)

corresponding to the state transition diagram, where $Q$ is the transition rates matrix of degree $N_{DC} + 2$ including the failure rate $\lambda_k$ and the repair rate $\mu_k = 1/MTTR_k$, $k = 1, 2, \ldots, N$. The initial condition is $p(0) = [1 \ 0 \ \cdots \ 0]^T$. Omit $N_{DC} + 2$-th row and $N_{DC} + 2$-th column of $Q$ to obtain $Q_0$ of degree $N_{DC} + 1$, and solve the linear equation

$$Q_0q(t) = [-1 \ 0 \ \cdots \ 0]^T$$  (18)

to obtain the solution $q = [q_0 \ q_1 \ \cdots \ q_{N_{DC}}]^T$. Since $q_k$ is equal to $\int_0^\infty p_k(t)dt$, which indicates the mean total dwell-time in $S_k$, MTTA (Mean Time To Absorption) until the system transits to the only absorbing state $S_{N_{DC} + 1}$ is obtained by

$$\text{MTTA} = \sum_{k=0}^{N_{DC}} q_k.$$  (19)

Under the reasonable assumption that the necessary time for measures after the deviations from the normal operating-range is sufficiently shorter than MTTA, the frequency of the deviations caused by the system destabilization is obtained by

$$\omega_{\text{unstable}}([i_1, i_2, \ldots, i_N]) = \frac{1}{\text{MTTA}} = \left(\sum_{k=0}^{N_{DC}} q_k\right)^{-1}.$$  (20)

It evaluates the dependability function in the control law to maintain the stability and the control performance not only in the normal operation but also under fault conditions. The dependability function is the basis of the safety function against the deviations from the normal operating-range.

Step 2-3: all representative safety functions satisfying dependability requirement Obtain the following set:

$$C_1 = \{[i_1, i_2, \ldots, i_N] \mid \omega_{\text{unstable}}([i_1, i_2, \ldots, i_N]) < DF_{\text{tar}}\}.$$  (21)

This is the set of all representative safety functions satisfying dependability requirement because $\omega_{\text{unstable}}$ evaluates dependability function to maintain the stability (and the control performance of the control system) even if the system is not in the normal operation.
4.3 Step 3: control law design

Obtain a new generalized plant $G$ as shown in Fig. 4(a) from the original one $G_{org}$ in Fig. 3. For each representative safety function $[i_1, i_2, \ldots, i_N] \in C_1$, its set of device contexts $S = \{S_1, S_2, \ldots, S_{N_{DC}}\}$. The fault-case control performance in the device context $S_i$ : $[\delta_1, \delta_2, \ldots, \delta_N]$ can be formulated as follows.

Define

$\Delta_i = \text{diag}\{\delta_{11}, \delta_{22}, \ldots, \delta_{NN}\}$

(22)

corresponding to $S_i$. Using $\Delta_i$, define a new generalized plant $G'_i$ as shown in Fig. 4(b). Then, the control system in $S_i$ is concretely described by

\[ F_i(G'_i, K) : \begin{cases} \frac{dx(t)}{dt} = A_i x(t) + B_i w(t) \\ z(t) = C_i x(t) + D_i w(t) \end{cases} \]

(23)

\[ A_i = \begin{bmatrix} A_G + B_{G2} \Delta_{si} D_K \Delta_{si} C_{G2} & B_{G2} \Delta_{si} C_K \\ B_K \Delta_{si} C_{G2} & A_K \end{bmatrix} \]

\[ B_i = \begin{bmatrix} B_{G1} + B_{G2} \Delta_{si} D_K \Delta_{si} D_{G21} \\ B_K \Delta_{si} D_{G21} \end{bmatrix} \]

\[ C_i = \begin{bmatrix} C_{G1} + D_{G12} \Delta_{si} D_K \Delta_{si} C_{G2} \\ D_{G12} \Delta_{si} C_K \end{bmatrix} \]

\[ D_i = D_{G11} + D_{G12} \Delta_{si} D_K \Delta_{si} D_{G21} \]

where $x(t) \in \mathbb{R}^n$ is the same internal state of the control system as in (6) and $\Delta_{si} = \text{diag}\{1 - \delta_{11}, 1 - \delta_{22}, \ldots, 1 - \delta_{NN}\}$, $\Delta_{si} = \text{diag}\{1 - \delta_{11}, 1 - \delta_{N_{DC}}, 1 - \delta_{N_{DC}} + \ldots, 1 - \delta_{NN}\}$. The normal-case control system (6) is the special case of (23) where $\Delta_0 = 0$. Then, the fault-case control performance in $S_i$ is obtained by

\[ \gamma_i = \|F_i(G'_i, K)\|_{\infty}. \]

(24)

Note that the normal-case control performance (5) is the special case of (24) where $\Delta_0 = 0$.

Next, suppose that the representative safety function $[i_1, i_2, \ldots, i_N] \in C_1$ has its set of all possible switchings $\Theta = \{\Theta_1, \Theta_2, \ldots, \Theta_{N_{SW}}\}$, where $N_{SW}$ denotes the number of them. The switching $\Theta_i : (l_1, l_2; k) \in \Theta$ implies that the uncertainty $\Delta$ is switched from $\Delta_{i_1}$ to $\Delta_{i_2}$ by the failure in Device $k$, and that the transfer function matrix of the closed-loop control system from $w(t)$ to $z(t)$ is switched from $F_i(G'_{i_1}, K)$ to $F_i(G'_{i_2}, K)$. The fluctuations of transient responses caused by the switching $\Theta_i$ are evaluated by the switching $L_2$ gain (Hespanha [2003], Sebe [2010]):

\[ \theta_j = \sup_{w(t) \in L_2(-\infty, \infty) \setminus \{0\}} \frac{\|z(t)\|_2}{\|w(t)\|_2}. \]

(25)

That is, the switching $L_2$ gain (25) is considered to be the performance index for the fluctuations of transient responses caused by a failure.

Note that the switching $L_2$ gain (25) does not depend on the switching time, i.e., the failure time (Sebe [2010]). It can be obtained under the assumption that the failure occurs at $t = 0$.

The worst $w(t)$ ($t \in (-\infty, \infty)$) corresponding to the switching $L_2$ gain is exactly amplified by the gain. The $t \in (-\infty, 0]$ part of the worst $w(t)$ realizes the worst system situation at $t = 0$ for the considered switching.

**Remark 3.** In a switching $\Theta_i : (l_1, l_2; k) \in \Theta$, if $S_i$, is not Normal, i.e., if the control system has already includes device faults when the switching occurs, we assume that the transient response caused by the previous failures has already converged to zero vanishingly at the switching time in order to evaluate properly the fluctuations of transient responses caused by the switching.

**Step 3-1: target response-fluctuation control performance**

Set a target response-fluctuation control performance, $\theta_{\text{tar}}$, so that

\[ \theta_{\text{tar}} \geq \bar{\theta} \]

(26)

is satisfied.

**Step 3-2: optimization**

Solve the optimization problem:

- minimize $\gamma_0$
- subject to $\gamma_i < \bar{\theta}$ ($i = 1, 2, \ldots, N_{DC}$)
- $\theta_j < \theta_{\text{tar}}$ ($j = 1, 2, \ldots, N_{SW}$)

(27)

by multiobjective design with the iterative performance improvement procedure using a non-common Lyapunov function presented in Sebe [2007] to obtain the optimal value of $\gamma_0, \gamma_0 = \gamma_0 ([i_1, i_2, \ldots, i_N])$, and the control law, $K = K ([i_1, i_2, \ldots, i_N])$, achieving it.

4.4 Step 4: all representative safety functions satisfying safety requirement

For each representative safety function $[i_1, i_2, \ldots, i_N] \in C_1$, obtain the frequency of the deviations caused by the fluctuations of transient responses of the control system with $K ([i_1, i_2, \ldots, i_N])$ obtained in Step 3. It evaluates the safety ability in the representative safety function to suppress the fluctuations of transient responses after a device failure in order to prevent the deviations.

**Step 4-1: frequency of deviations caused by fluctuations of transient responses**

For each representative safety function $[i_1, i_2, \ldots, i_N] \in C_1$ with its set of all possible switchings $\Theta = \{\Theta_1, \Theta_2, \ldots, \Theta_{N_{SW}}\}$, consider that the switching $\Theta_j : (l_1, l_2; k) \in \Theta$ occurs at $t = 0$ without loss of
generality. Suppose that by the same internal state $x(t) \in \mathbb{R}^n$ as in the normal-case state equation (6), the control system before the switching, i.e., in $S_{l_1}$ in Normal/S, is described by

$$\begin{cases}
\frac{dx(t)}{dt} = A_{l_1}x(t) + B_{l_1}w(t) \\
z(t) = C_{l_1}x(t) + D_{l_1}w(t)
\end{cases} \quad (t \leq 0) \quad (28)$$

and the control system after the switching, i.e., in $S_{l_2} \in S$, is described by

$$\begin{cases}
\frac{dx(t)}{dt} = A_{l_2}x(t) + B_{l_2}w(t) \\
z(t) = C_{l_2}x(t) + D_{l_2}w(t)
\end{cases} \quad (t > 0) \quad (29)$$

(see (23)). There exists the antistabilizing solution $X_{l_1} > O$ to the Riccati equation

$$X_{l_1}A_{l_1} + A_{l_1}^TX_{l_1} + C_{l_1}^TC_{l_1} + (X_{l_1}B_{l_1} + C_{l_1}^TD_{l_1}) \times (\overline{\Theta}^2I - D_{l_1}^TD_{l_1})^{-1}(X_{l_1}B_{l_1} + C_{l_1}^TD_{l_1})^T = 0 \quad (30)$$

because $\gamma_l < \overline{\Theta}$. Also there exists the stabilizing solution $X_{l_2} > O$ to the Riccati equation

$$X_{l_2}A_{l_2} + A_{l_2}^TX_{l_2} + C_{l_2}^TC_{l_2} + (X_{l_2}B_{l_2} + C_{l_2}^TD_{l_2}) \times (\overline{\Theta}^2I - D_{l_2}^TD_{l_2})^{-1}(X_{l_2}B_{l_2} + C_{l_2}^TD_{l_2})^T = 0 \quad (31)$$

because $\gamma_l < \overline{\Theta}$. Define

$$X_j = X_{l_1} - X_{l_2}. \quad (32)$$

Let $U_{B_n}$ denote the surface of the unit ball in the internal state space $x \in \mathbb{R}^n$ as follows:

$$U_{B_n} = \{ x \in \mathbb{R}^n \mid x^Tx = 1 \}. \quad (33)$$

Consider the following region on $U_{B_n}$:

$$R_j = \{ x \in U_{B_n} \mid x^Tx_j < 0 \}. \quad (34)$$

According to Sebe [2010], if the internal state of the control system at the switching is in the direction of $x_0 \in R_j$, i.e., there exist $c > 0$ and $x_0 \in R_j$ such that $x(0) = c \cdot x_0$, there is the possibility that $\| z(t) \| > \overline{\Theta}$. Whether $\| z(t) \| > \overline{\Theta}$ actually, i.e., there is the possibility that deviations from the normal operating-range occur, depends on the exogenous input after the switching, $w(t)$ ($t > 0$).

Assumption 6. The distribution of the direction of the internal state in the normal operation and in the intermediate device contexts is probabilistically uniform. The surface area of $U_{B_n}$ is obtained by

$$S_n = \frac{n \cdot \pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2} + 1)} \quad (35)$$

where $\Gamma$ denotes the gamma function. Hence, under Assumption 6, the probability that the internal state of the control system at the switching $\Theta_j : (i_1, i_2) \in \Theta$, is in the direction of the region $R_j$ is obtained by

$$P_j = \frac{1}{S_n} \int_{R_j} dx \quad (36)$$

where $\int_{R_j} dx$ denotes the surface area of $R_j$ on $U_{B_n}$.

Remark 4. The deviations do not always occur even if the switching $\Theta_j$ occurs when the internal state of the control system is in the direction of the region $R_j$. Hence this analysis gives conservative evaluation.

On the other hand, in Step 2-2, for each switching $\Theta_j : (i_1, i_2; k) \in \Theta$, its occurrence frequency is obtained by

$$\omega_j = \lambda_k \cdot \frac{q_l}{\text{MTTA}}. \quad (37)$$

Then, the frequency of the deviations caused by the fluctuations of transient responses is obtained by

$$\omega_{\text{resp}}(i_1, i_2, \ldots, i_N) = \sum_{j=1}^{N_{\text{SW}}} \omega_j P_j. \quad (38)$$

Step 4-2: demand frequency From $\omega_{\text{unstable}}$ obtained in Step 2 and $\omega_{\text{resp}}$ obtained in Step 4-1, the demand frequency is obtained by

$$\text{DF}(i_1, i_2, \ldots, i_N) = \omega_{\text{unstable}}(i_1, i_2, \ldots, i_N) + \omega_{\text{resp}}(i_1, i_2, \ldots, i_N). \quad (39)$$

The safety function in the control law $K(i_1, i_2, \ldots, i_N)$ against the deviations from the normal operating-range can be evaluated by this value of $\text{DF}(i_1, i_2, \ldots, i_N)$.

Step 4-3: all representative safety functions satisfying safety requirement Obtain the following set of all representative safety functions satisfying safety requirement:

$$C_2 = \{ i_1, i_2, \ldots, i_N \in C_1 \mid \text{DF}(i_1, i_2, \ldots, i_N) < \text{DF}_{\text{tar}} \}. \quad (40)$$

4.5 Step 5: conclusive solution

The conclusive solution is obtained by

$$\min_{[i_1, i_2, \ldots, i_N] \in C_2} \hat{\gamma}_0([i_1, i_2, \ldots, i_N]) \quad (41)$$

and the corresponding control law $K(i_1, i_2, \ldots, i_N)$.

Remark 5. If we set a target response-fluctuation performance $\theta_{\text{tar}}$ as $\theta_{\text{tar}} = \overline{\Theta}$ in Step 3-1,

$$\omega_{\text{resp}}([i_1, i_2, \ldots, i_N]) = 0 \quad (42)$$

hence

$$\text{DF}(i_1, i_2, \ldots, i_N) = \omega_{\text{unstable}}(i_1, i_2, \ldots, i_N) \quad (43)$$

for each representative safety function $[i_1, i_2, \ldots, i_N] \in C_1$ (see Suyama [2010]). Then Step 4 is not necessary for obtaining the conclusive solution

$$\min_{[i_1, i_2, \ldots, i_N] \in C_1} \hat{\gamma}_0([i_1, i_2, \ldots, i_N]) \quad (44)$$

because $C_1 = C_2$.

5. EXAMPLE

Consider the following generalized plant:

$$\begin{bmatrix}
\dot{z} \\
y
\end{bmatrix} = \begin{bmatrix}
-2 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
3 & 0 & 0 & 2 & 0 & 1 & 0 & 1 & 0 \\
-1 & 0 & -2 & -3 & 1 & 0 & 0 & 1 & 0 \\
-2 & -1 & -2 & -1 & 1 & 0 & 1 & 0 & 1 \\
-1 & 2 & -1 & 0 & 0 & 0 & 1 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0
\end{bmatrix} \begin{bmatrix}
w \\
u
\end{bmatrix}. \quad (36)$$

In this case $N_a = 3$, $N_a = 3$, $N = 6$. The failure rates and MTTRs of Sensors 1, 2 and 3 (Devices 1, 2 and 3) and Actuators 1, 2 and 3 (Devices 4, 5 and 6) are as follows:
Table 2. Design result.

<table>
<thead>
<tr>
<th>Class</th>
<th>Step 2: Number of representative safety functions</th>
<th>Step 3</th>
<th>Step 4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Representative safety function</td>
<td>$\omega_{unstable}$</td>
<td>$\gamma_0$</td>
</tr>
<tr>
<td>$&lt;1,0,0,0,0,0&gt; = 63$</td>
<td>$2$</td>
<td>${1,1,1,1,0,1}$</td>
<td>$9.3180 \times 10^{-6} [1/hr]$</td>
</tr>
<tr>
<td>$&lt;1,1,0,0,0,0&gt; = 240$</td>
<td>$25$</td>
<td>${2,1,1,2,0,1}$</td>
<td>$8.6863 \times 10^{-6} [1/hr]$</td>
</tr>
<tr>
<td>$&lt;1,2,0,0,0,0&gt; = 180$</td>
<td>$60$</td>
<td>${1,1,1,0,1,0}$</td>
<td>$8.6863 \times 10^{-6} [1/hr]$</td>
</tr>
<tr>
<td>$&lt;0,0,0,0,0,1&gt; = 15$</td>
<td>$15$</td>
<td>${1,1,1,0,1,0}$</td>
<td>$8.6863 \times 10^{-6} [1/hr]$</td>
</tr>
<tr>
<td>$&lt;1,0,1,0,0,0&gt; = 60$</td>
<td>$22$</td>
<td>${2,1,1,2,0,1}$</td>
<td>$8.6863 \times 10^{-6} [1/hr]$</td>
</tr>
<tr>
<td>$&lt;1,0,0,0,1,0&gt; = 12$</td>
<td>$9$</td>
<td>${1,1,1,0,1,0}$</td>
<td>$8.6863 \times 10^{-6} [1/hr]$</td>
</tr>
<tr>
<td>Total number</td>
<td>$876$</td>
<td>$259$</td>
<td></td>
</tr>
</tbody>
</table>

Table 3. Comparison among design methods.

<table>
<thead>
<tr>
<th>Design method</th>
<th>$\gamma_0$</th>
<th>$\max \gamma_i$</th>
<th>$\max \delta_i$</th>
<th>$\omega_{unstable}$</th>
<th>$\omega_{resp}$</th>
<th>DF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method in Asai [2000]</td>
<td>$0.68621$</td>
<td>$1.08556$</td>
<td>$1.08556$</td>
<td>$1.1400 \times 10^{-4} [1/hr]$</td>
<td>$0.0116$</td>
<td>$1.1400 \times 10^{-4} [1/hr]$</td>
</tr>
<tr>
<td>Optimization (46)</td>
<td>$0.07261$</td>
<td>$0.19999$</td>
<td>$0.28561$</td>
<td>$9.3180 \times 10^{-6} [1/hr]$</td>
<td>$7.9801 \times 10^{-7} [1/hr]$</td>
<td>$0.1016 \times 10^{-6} [1/hr]$</td>
</tr>
<tr>
<td>Proposed design</td>
<td>$0.07732$</td>
<td>$0.19995$</td>
<td>$0.19995$</td>
<td>$9.3180 \times 10^{-6} [1/hr]$</td>
<td>$0$</td>
<td>$9.3180 \times 10^{-6} [1/hr]$</td>
</tr>
</tbody>
</table>

Suppose that $\|w(t)\|_2 \leq 1 (= \pi)$. In Remark 1, the normal operating-ranges of $z(t)$ is $[-0.4, 0.4]$. The sufficiently short time-interval just after a failure is set by $T_0 = 0.25$ in consideration of the worst transient responses in some switchings such as shown in Fig. 5, which should be obtained beforehand. Then it follows from (10) that $\bar{T} = 0.2$. Hence it is assumed that the deviations from the normal operating-range occur only when $\|z(t)\| > 0.2$.

Set $DF_{tar} = 1 \times 10^{-5} [1/hr]$ so that $HEF_{tar} = 10^{-3} [1/yr]$ can be achieved by only one E/E/PE SRS of SIL2 in low demand mode of operation with an enough margin.

Step 1: $\bar{\gamma} = 0.2/1 = 0.2$.

Step 2: A total of 876 representative safety functions can be considered as shown in Table 2. A total of 259 representative safety functions satisfy the dependability requirement $\omega_{unstable} < DF_{tar}$ as shown in Table 2, which are the elements of the set $C_1$.

Step 3: We set a target response-fluctuation performance by $\theta_{tar} = 0.2$ ($= \bar{\gamma}$).

For each representative safety function $[i_1, i_2, \ldots, i_6] \in C_1$, we do the optimization (27). Then two representative safety functions, $[1,1,1,1,0,1]$ and $[2,1,1,2,0,1]$, satisfy $\gamma_0 < 0.2$ as shown in Table 2.

Step 4: In Step 3-1 we set $\theta_{tar} = \bar{\gamma}$, then $DF = \omega_{unstable}$ for the representative safety functions belonging to the set $C_1$ as shown in Table 2. Hence the set $C_2$ of all representative safety functions satisfying the safety requirement $DF < DF_{tar}$ is equivalent to the set $C_1$. See Remark 5.

Step 5: The conclusive solution is the following control law achieving representative safety function $[1,1,1,1,0,1]$ and the optimal normal-case control performance $0.07732$:

\[
K = \begin{bmatrix}
-1845 & -844.7 & -1460 & 116.9 & -109.7 & 202.1 & -459.9 \\
113.9 & 76.51 & 87.52 & -8.373 & 7.224 & -13.46 & 28.97 \\
1460 & 872.7 & 113.4 & -99.35 & 92.82 & -167.9 & 368.7 \\
545.9 & 189.1 & 438.7 & -36.49 & 28.33 & -57.42 & 134.6 \\
35.93 & -52.92 & 34.50 & 2.794 & -0.8958 & -2.365 & 7.050 \\
1323 & 220.4 & 1089 & -77.68 & 65.07 & -130.5 & 320.6 \\
289.7 & -271.9 & 269.4 & -2.502 & 1.766 & -15.93 & 64.55
\end{bmatrix}
\]
To clarify the effect of suppress the fluctuations of transient responses after a failure, compare the above design with the following two designs dealing with the same set of device contexts corresponding to \([1, 1, 1, 1, 0, 1]\).

- Method in Asai [2000]: optimization
  
  \[
  \min_k \max_j \{\gamma_0, \gamma_1, \gamma_2, \ldots, \gamma_{N_{DC}}\}. \tag{45}
  \]

- Optimization
  
  \[
  \min_k \gamma_0 \text{ subject to } \gamma_i < 0.2 \ (i = 1, 2, \ldots, N_{DC}). \tag{46}
  \]

Table 3 shows the performance indices in the designs. Figure 5 shows the worst transient response for each design at the switching from Normal to \((0, 0, 1, 0, 0, 0)\) by a failure in Device 3 at \(t = 0\). The worst \(w(t) \ (t \in (-\infty, 0])\) for each design realizes the worst direction of the internal state at \(t = 0\) (Sebe [2010], Suyama [2010]).

Since the optimization (45) is based on the common Lyapunov function in Asai [2000], the normal-case control performance \(\gamma_0\) and the fault-case control performances \(\max \gamma_i\) are not desirable as \(\gamma_0, \max_i \gamma_i > \overline{\theta}\). Since \(\gamma_1, \gamma_2 \leq \theta_j\) at the switching \(\Theta_j = (l_1, l_2, k)\), all device contexts are regarded as unstable states in the safety assessment, i.e., \(S = \psi\), while the control system is stable actually in device contexts corresponding to the representative safety function \([1, 1, 1, 1, 0, 1]\) such as \((1, 0, 0, 0, 0, 0), (0, 1, 0, 0, 0, 0)\), and so on. That is, in the sense of the system safety, such a system is equivalent to the system falling into an unstable state even if one device fails (Suyama [2010]).

Hence \(\omega_{\text{unstable}} = \sum_{k=1}^{N_{DC}} \lambda_k\) and there is no need to consider the possible deviations from the normal operating-range caused by the fluctuations of transient responses after a failure, i.e., \(\omega_{\text{resp}}\). In fact, the deviation occurs against the worst \(w(t)\) at the switching from Normal to \((0, 0, 1, 0, 0, 0)\) by a failure in Device 3 as shown in Figure 5. In the design by the optimization (46) without considering the response-fluctuation performance, where no measures for suppressing the fluctuations of transient responses are taken into consideration, the normal-case control performance is better than that in the proposed design, while the response-fluctuation performance is worse as \(\max_j \theta_j > \overline{\theta}\). Hence the deviation occurs against the worst \(w(t)\), for example, at the switching from Normal to \((0, 0, 1, 0, 0, 0)\) by a failure in Device 3 as shown in Figure 5. As a result, \(DF = \omega_{\text{unstable}} + \omega_{\text{resp}} > DF_{\text{tar}}\) due to \(\omega_{\text{resp}}(> 0)\). It implies that the design by the optimization (46) does not satisfy the safety requirement.

In the proposed design with \(\theta_{\text{tar}} = \overline{\theta}\), \(\max_j \theta_j < \overline{\theta}\). The deviations do not occur even against the worst \(w(t)\) at all possible switchings due to the safety ability to suppress the fluctuations of transient responses as shown in Figure 5. As a result, the safety requirement \(DF < DF_{\text{tar}}\) is satisfied, while the normal-case control performance is optimized. Note that, even if we set \(\theta_{\text{tar}} > \overline{\theta}\), the proposed framework gives a design satisfying the safety requirement.

6. CONCLUSION

This paper has proposed the realization of safety function in control laws to reduce the frequency of events that a physical value in a control system deviates from its normal operating-range. The safety function consists of

- the safety ability to suppress the fluctuations of transient responses after a device failure, and
- the dependability function to maintain the stability and the control performance of the control system even if the system is not in the normal operation.

The safety function in control laws can supplement ordinary safety-related systems in risk reduction according to international safety standards such as IEC 61508, where its contribution can be evaluated quantitatively.

The distinction between safety and dependability is quite important widely in system analysis and design according to international standards. This is the first study in fault-tolerant control based on the strict distinction authorized by international standards.

ACKNOWLEDGEMENT

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

REFERENCES