Proceeding of the 2004 American Control Conference
Boston, Massachusetts June 30 - July 2, 2004

# Controller design using safety performance index according to IEC 61508

Koichi Suyama
Tokyo University of Marine Science and Technology
Etchujima, Koto-ku, Tokyo 135-8533, Japan

*Abstract*— **This paper presents a controller design framework using a performance index for control system safety. The presented index and the framework are based on the contribution of reliable control theory to system safety design according to the international safety standard, IEC 61508. It clarifies that control system safety is one of most important control performances.**

## I. INTRODUCTION

Over the past decade the social environment surrounding system safety has changed rapidly, as seen in [5]. One of the epochs was that TC65 WG9&10 in IEC, International Electrotechnical Commission, established an international standard, IEC 61508[7]. It is applied to almost all electrical/electronic/programmable electronic safety-related systems irrespective of their applications. It has been already quoted into several national standards or guidelines of UK, USA and Japan, including those for process, aerospace and railway transportation sectors.

On the other hand, since Šiljak firstly used the term *reliable control* in the field of control theory in the late 1970s, many studies have simultaneously and independently been made on control system design under possible device failures, such as integrity[1], [3], [11], [4], reliable $H_\infty$ control[19], [20], [22], [23], [24], [25] and passive redundancy[21], [10], [14].

The importance of safety function realized in a control system has been growing for the last several years. One of the reasons is that ISO/IEC Guide 51 (E)[9] adopted newly risk for environment and risk for properties as its scope. It is widely known that there are many cases where safety measures outside a control system are not enough to reduce the risk for environment/properties. Hence reliable control has been brought to attention by its contribution to system design according to IEC 61508, which can achieve safety function in a control system[16], [17].

The author has presented a safety integrity analysis framework for a controller designed especially by reliable control according to the international safety standard, IEC 61508 [18]. The presented framework clarifies a concrete contribution of reliable control to required risk reduction and an established meaning of reliable control in system safety design according to IEC 61508. Hence almost all reliable control can be included to the international standard system.

This paper presents a controller design framework using a safety performance index. The presented index and the framework are based on the contribution of reliable control theory to system safety design according to IEC 61508. It clarifies that control system safety is one of most important control performances.

IEC 61508 is now under maintenance. In the maintenance a safety evaluation framework for software used in safety-related systems will newly be prepared. The content of a controller is a control logic. Hence, if we design safety function in a controller, of course, we should set a target safety integrity as one of control performance indices to achieve in controller design.

## II. IEC 61508

Safety has been considered in the sense of probabilistic risk until ISO/IEC Guide 51[8] was established. In IEC 61508, safety measures are evaluated probabilistically from a standpoint of risk reduction according to ISO/IEC Guide 51.

Figures 1 and 2 illustrate the overall system configuration and its risk reduction considered in IEC 61508. The original control system consists of

- Equipment Under Control (EUC): equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities, and
- Basic Control System (BCS): system which responds to input signals from the process and/or an operator and generates output signals causing the EUC to operate in the desired manner.

IEC 61508 requests to reduce the initial risk of the original control system by the following measures so that the residual risk of the overall system is less than the predetermined tolerable risk level.

- Safety-Related Systems (SRSs): systems that implement the required safety functions necessary to achieve or to maintain a safe state for the EUC.
  - Electrical / electronic / programmable electronic (E/E/PE) SRSs: SRSs based on E/E/PE technology.
  - Other technology SRSs: SRSs based on other technologies, e.g., a safety valve.
- External Risk Reduction Facilities (ERRFs): physical measures taken external to SRSs to reduce or mitigate the risk, e.g., bunds around flammable liquid storage tanks.

0-7803-8335-4/04/$17.00 ©2004 AACC

To be precise, IEC 61508 is the international standard for E/E/PE SRSs.

A SRS, just like a safety device, has safety function to achieve or to maintain a safe state of the EUC. Functional safety is its ability to perform the safety function.

Note that a hardware failure occurs at a random time in a SRS. Then there is the possibility that the SRS cannot perform its safety function. IEC 61508 evaluates functional safety of an E/E/PE SRS, i.e., the probability of failure to perform its safety function, using four safety integrity levels (SILs) for two kinds of operation modes shown in Table 1. If a SRS shoulders a heavy burden for risk reduction, it is required to fit a higher SIL.

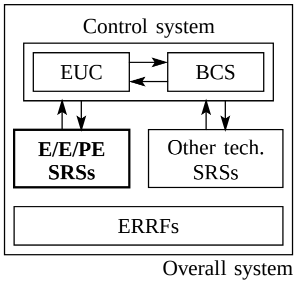

Figure 1. Overall system.

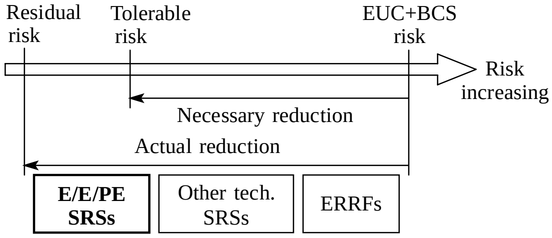

Figure 2. Risk reduction.

Table 1. Safety integrity levels.

(a) Low demand mode of operation.

| SIL | Average probability of failure to perform its design function on demand |
|---|---|
| 4 | $\geq 10^{-5}$ to $< 10^{-4}$ |
| 3 | $\geq 10^{-4}$ to $< 10^{-3}$ |
| 2 | $\geq 10^{-3}$ to $< 10^{-2}$ |
| 1 | $\geq 10^{-2}$ to $< 10^{-1}$ |

(b) High demand / continuous mode of operation.

| SIL | Probability of a dangerous failure per hour |
|---|---|
| 4 | $\geq 10^{-9}$ to $< 10^{-8}$ |
| 3 | $\geq 10^{-8}$ to $< 10^{-7}$ |
| 2 | $\geq 10^{-7}$ to $< 10^{-6}$ |
| 1 | $\geq 10^{-6}$ to $< 10^{-5}$ |

IEC 61508 applies SILs in high demand / continuous operation mode shown in Table 1(b) to a SRS inside a control system, i.e., inside a BCS. If the probability of a dangerous failure, where safety function realized by reliable control in a BCS is lost, is less than $10^{-5}[1/\text{hour}]$, the BCS itself is regarded as a SRS. Then IEC 61508 should be applied to the BCS.

## III. Contribution of reliable control to risk reduction according to IEC 61508

Reliable control realizes safety function against device failures in the redundancy in the sense of productivity or efficiency existing in a control system at the sacrifice of the normal-case control performance[16], [17]. Because it is sufficient that risk reduction shown in Figure 2 is achieved as the overall system shown in Figure 1, the safety function achieved by reliable control can be complementary to SRSs as shown in Figure 3.

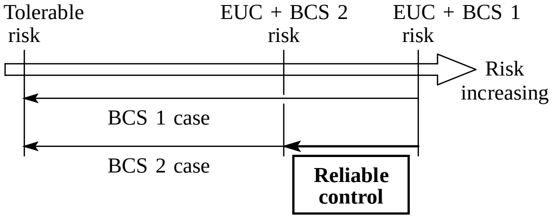

Figure 3. Necessary risk reduction.

Due to the functional safety realized by reliable control, the risk of the control system EUC + BCS 2 obtained is less than the risk of EUC + BCS 1 obtained by an ordinary controller design. Hence, when we reduce the risk of the overall system so that the residual risk is less than the tolerable risk, a lighter burden is imposed on SRSs in the EUC + BCS 2 case. For example, we can imagine that a SRS of SIL 2 is sufficient for the control system EUC + BCS 2 while the control system EUC + BCS 1 needs a SRS of SIL 3 or 4.

## IV. Controller design framework using safety performance index

### A. Safety performance index

Consider a control system shown in Figure 4, where Sensor 1, …, Sensor $N_s$ and Actuator 1, …, Actuator $N_a$ are used. Let Device 1, …, Device $N$ denote them, where $N = N_s + N_a$.

**Assumption 1**: A failure, a functional stoppage, probabilistically occurs in Device $i$ in accordance with the exponential distribution with the failure rate $\lambda_i$, $i = 1, \ldots, N$.

This is an ordinary assumption in the field of safety/reliability engineering.

**Assumption 2**:

(a) A demand on an E/E/PE SRS occurs when the control system falls into an unstable state.

(b) The demand frequency is no greater than one per year and no greater than twice the preventive maintenance frequency.

Assumption 2(b) indicates the low demand mode of operation in IEC 61508 and makes the meaning of the presented evaluation framework clear.

**Remark 1**: The presented framework can be extended to a more general one by taking the following into consideration:

- stability degree, or
- threshold on control performance for all device situations.

However, in general, we should set up criteria for demand occurrences by considering the detection ability of an E/E/PE SRS. Hence, in this paper, we study the most basic case by Assumption 2(a).

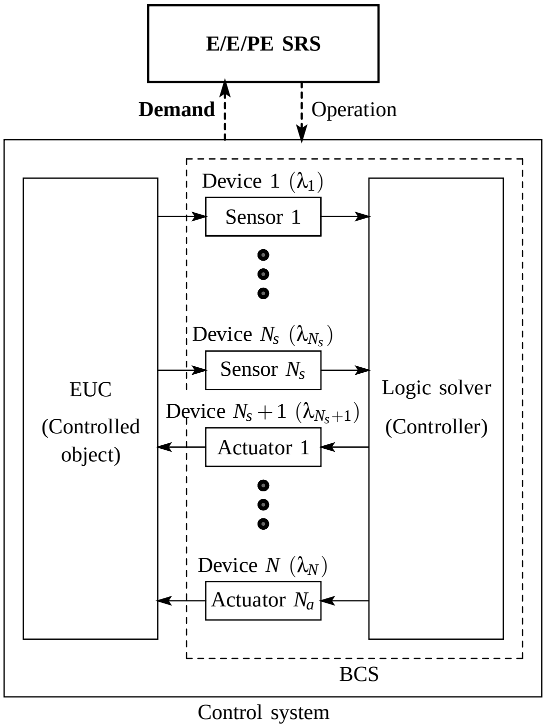

Figure 4. Control system and SRS.

The safety performance index, which plays an essential role in the presented controller design framework, is demand frequency of the resulting control system. The demand frequency itself is used for E/E/PE SRS design achieving a given target safety integrity level, i.e., target hazard frequency. It reflects the safety integrity of a controller realized by reliable control theory, as presented in [18].

## B. Controller design framework

Figure 5 illustrates the presented controller design framework based on the safety performance index, demand frequency. It consists of the following steps:

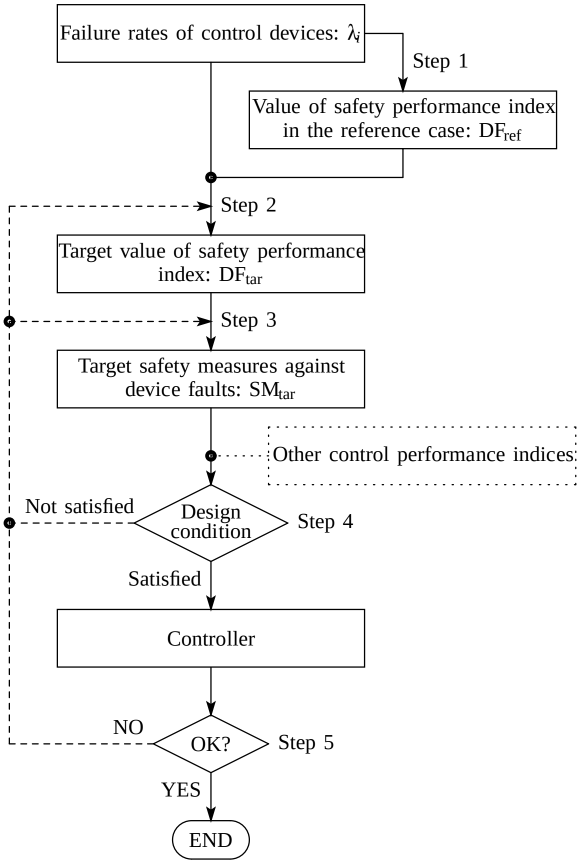
Failure rates of control devices: $\lambda_i$
Step 1
Value of safety performance index in the reference case: $\mathrm{DF}_{\mathrm{ref}}$
Step 2
Target value of safety performance index: $\mathrm{DF}_{\mathrm{tar}}$
Step 3
Target safety measures against device faults: $\mathrm{SM}_{\mathrm{tar}}$
Other control performance indices
Not satisfied
Design condition
Step 4
Satisfied
Controller
NO
OK?
Step 5
YES
END

Figure 5. Controller design framework using a safety performance index.

Step 1: obtain the demand frequency in the reference case
Step 2: set a target demand frequency using the information obtained in Step 1
Step 3: obtain target safety measures against device faults achieving the target demand frequency set in Step 2
Step 4: design a controller satisfying the safety measures against device faults obtained in Step 3 and other control performance indices, if any, by reliable control theory
Step 5: evaluation of the controller obtained in Step 4.

*1) Step 1: analysis of reference case:* Consider the reference case where the control system falls into an unstable state and a demand on an E/E/PE SRS occurs if only one device fails. That is, such a controller, i.e., a control logic, without any safety functions is used.

Define

$$\lambda_{\mathrm{all}} = \sum_{i=1}^{N} \lambda_i. \tag{1}$$

Then, the demand rate in this reference case is

$$\mathrm{DR}_{\mathrm{ref}} = \lambda_{\mathrm{all}} \tag{2}$$

and the mean time to demand in this reference case is

$$\mathrm{MTTD}_{\mathrm{ref}} = \frac{1}{\lambda_{\mathrm{all}}}. \tag{3}$$

In general, a demand frequency is given by

$$\mathrm{DF} = \frac{1}{\frac{1}{\mathrm{DR}} + (\text{SRS operation time}) + \mathrm{MTTR}} \tag{4}$$

where MTTR denotes a mean time to repair.

**Assumption 3**:

$$\frac{1}{\mathrm{DR}} \gg (\text{SRS operation time}) + \mathrm{MTTR}. \tag{5}$$

Under this reasonable assumption, the demand frequency in this reference case is

$$\mathrm{DF}_{\mathrm{ref}} = \lambda_{\mathrm{all}}. \tag{6}$$

This indicates the safety integrity of a controller without any safety functions, which should be compared with the safety integrity of a controller design by reliable control theory.

*2) Step 2: target demand frequency:* Set a target demand frequency $\mathrm{DF}_{\mathrm{tar}}$ satisfying $\mathrm{DF}_{\mathrm{tar}} < \mathrm{DF}_{\mathrm{ref}}$.

Functional safety of an E/E/PE SRS in the low demand mode of operation is evaluated by average probability of failure to perform its design function on demand (PFD). Here, a hazard frequency, HF, is given by

$$\mathrm{HF} = \mathrm{DF} \times \mathrm{PFD} \tag{7}$$

where DF denotes demand frequency. Hence, given a target hazard frequency, $\mathrm{HF}_{\mathrm{tar}}$, we can obtain a required PFD by

$$\mathrm{PFD}_{\mathrm{req}} \leq \frac{\mathrm{HF}_{\mathrm{tar}}}{\mathrm{DF}} \tag{8}$$

and a required SIL, $\mathrm{SIL}_{\mathrm{req}}$, by Table 1(a). We should install an E/E/PE SRS of $\mathrm{SIL}_{\mathrm{req}}$.

Hence, taking $\mathrm{HF}_{\mathrm{tar}}$ and $\mathrm{PFD}_{\mathrm{req}}$, i.e., $\mathrm{SIL}_{\mathrm{req}}$, into consideration, we should set $\mathrm{DF}_{\mathrm{tar}}$.

Of course, the lower demand frequency, the better controller in the sense of system safety. It is because a E/E/PE SRS shoulders a light burden for risk reduction, i.e., it is required to fit a lower SIL. This is the concrete contribution of reliable control to IEC 61508.

*3) Step 3: target safety measures against device faults:* Each device is in either of two states, normal state: 0 and fault: 1. Hence, as a whole, the control system with $N$ devices is in one of $2^N$ device normal/fault situations. Represent safety measures against device fault situations to be achieved by reliable control design as follows:

$$\mathrm{SM} = \{\mathrm{DS}_1, \mathrm{DS}_2, \ldots\} \tag{9}$$

where

$$\mathrm{DS}_j = \{i_{j,1}, \ldots, i_{j,m_j}\}, \quad i_{j,k} \in \{1, 2, \ldots, N\}. \tag{10}$$

Here $\mathrm{DS}_j$, $j = 1, 2, \ldots$, is a set of device numbers and it means a set of safety measures such that the total control system maintains its stability even if a possible combination of device faults in the set occurs. Then

$$\mathrm{NSM} = \{1, 2, \ldots, N\} \setminus \cup_j \mathrm{DS}_j \tag{11}$$

is a set of device numbers which safety measures are not taken against their faults.

For example, in case $N = 5$,

$$\mathrm{SM} = \{\{1\}, \{3, 4, 5\}\}$$

denotes a set of safety measures such that the total control system maintains its stability in the following situations:

- Only Device 1 is in a fault
- Possible combinations of Devices 3, 4 and 5 are in faults
  - Only Device 3 is in a fault
  - Only Device 4 is in a fault
  - Only Device 5 is in a fault
  - Only Devices 3 and 4 are in faults
  - Only Devices 3 and 5 are in faults
  - Only Devices 4 and 5 are in faults
  - Only Devices 3, 4 and 5 are in faults.

No safety measures are taken against situations where Device 2 is in a fault.

**Assumption 4**:

$$\mathrm{DS}_{j_1} \cap \mathrm{DS}_{j_2} = \phi, \quad j_1 \neq j_2. \tag{12}$$

For $\mathrm{DS}_j$ in (10) define

$$a_{\mathrm{DS}_j} = \sum_{k \notin \mathrm{DS}_j} \lambda_k = \sum_{k \neq i_{j,1}, \ldots, i_{j,m_j}} \lambda_k. \tag{13}$$

Then the mean time to demand of a system with the safety measure (9) satisfying Assumption 4 is given by

$$\mathrm{MTTD(SM)} = \sum_j \left[ \frac{1}{a_{\mathrm{DS}_j}} - \frac{a_{\mathrm{DS}_j}}{\lambda_{\mathrm{all}}^2} \right] + \sum_{k \in \mathrm{NSM}} \frac{\lambda_k}{\lambda_{\mathrm{all}}^2}. \tag{14}$$

Hence, under Assumption 3, the demand frequency is given by

$$\mathrm{DF(SM)} = \frac{1}{\mathrm{MTTD(SM)}} = \frac{1}{\sum_j \left[ \frac{1}{a_{\mathrm{DS}_j}} - \frac{a_{\mathrm{DS}_j}}{\lambda_{\mathrm{all}}^2} \right] + \sum_{k \in \mathrm{NSM}} \frac{\lambda_k}{\lambda_{\mathrm{all}}^2}}. \tag{15}$$

*Outline of proof of (14)*: In (14), $\frac{1}{a_{\mathrm{DS}_j}} - \frac{a_{\mathrm{DS}_j}}{\lambda_{\mathrm{all}}^2}$ corresponds to demand occurrence scenarios where a first fault occurs in one of the devices included in $\mathrm{DS}_j$. Also $\frac{\lambda_k}{\lambda_{\mathrm{all}}^2}$ corresponds to the demand occurrence scenarios where the first fault occurs in Device $k$ included in NSM, i.e., no safety measures are taken against a fault in Device $k$, and the control system falls into an unstable state immediately.

For the target demand frequency set in Step 2, $\mathrm{DF}_{\mathrm{tar}}$, we can find target safety measures $\mathrm{SM}_{\mathrm{tar}}$ such that $\mathrm{DF}(\mathrm{SM}_{\mathrm{tar}}) \leq \mathrm{DF}_{\mathrm{tar}}$.

*4) Step 4: controller design by reliable control theory:* By reliable control theory, we design a controller such that

- it achieves the target safety measures $\mathrm{SM}_{\mathrm{tar}}$ obtained in Step 3, i.e., the resulting total control system maintains its stability even if the situation which $\mathrm{SM}_{\mathrm{tar}}$ supposes, and
- it achieves desirable values in other control performance indices, if any.

Of course there are cases

- where reliable control theory is not applicable to such design with the target safety measures $\mathrm{SM}_{\mathrm{tar}}$, e.g., reliable $H_\infty$ control cannot treat simultaneous faults in sensors and actuators efficiently, or
- (even if applicable) where there does not exist a solution to such a design problem with $\mathrm{SM}_{\mathrm{tar}}$.

In such cases we should return to Step 3 to change $\mathrm{SM}_{\mathrm{tar}}$. Furthermore, if necessary, we should return to Step 2 to change $\mathrm{DF}_{\mathrm{tar}}$.

*5) Step 5: controller evaluation:* As a final step, we should evaluate the controller obtained in Step 4 by the safety integrity analysis framework presented in [18].

## V. Example

Consider a control system consisting of a controlled object, three sensors, Sensor 1 (Device 1), Sensor 2 (Device 2) and Sensor 3 (Device 3), two actuators, Actuator 1 (Device 4) and Actuator 2 (Device 5), and a control logic. Suppose that

$$\begin{aligned}\lambda_1 &= 2.00\times 10^{-5}[1/\mathrm{hour}]\\ \lambda_2 &= 1.00\times 10^{-5}[1/\mathrm{hour}]\\ \lambda_3 &= 5.00\times 10^{-5}[1/\mathrm{hour}]\\ \lambda_4 &= 2.00\times 10^{-5}[1/\mathrm{hour}]\\ \lambda_5 &= 5.00\times 10^{-5}[1/\mathrm{hour}].\end{aligned}$$

The plant consisting of the controlled object, the three sensors, and the two actuators can be represented by

$$\begin{aligned}\frac{d}{dt}x(t) &= \begin{bmatrix} 0 & 1 & 1\\ 1 & 1 & 2\\ 1 & 1 & 1\end{bmatrix} x(t) + \begin{bmatrix} 1 & 0\\ 0 & 0\\ 0 & 1\end{bmatrix} u(t)\\ &\quad + \begin{bmatrix} 1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix} w(t)\\ y(t) &= x(t)\\ z(t) &= \begin{bmatrix} 2 & 2 & 0\\ 1 & 0 & 1\end{bmatrix} x(t) + \begin{bmatrix} 1 & 0\\ 0 & 1\end{bmatrix} w(t)\end{aligned}$$

where $w(t)$, $z(t)$ are the noise, and the performance output. Consider the disturbance attenuation performance evaluated by $\|T_{zw}\|_2$ where $T_zw$ is the transfer function from $w(t)$ to $z(t)$, and $\|\cdot\|_2$ denotes $H_2$-norm. We design state feedback

$$u(t) = Fx(t)$$

where the gain matrix $F$ is the essence of the control logic to be designed.

### *A. Step 1: analysis of reference case*

Solving a full-information two-block $H_2$ problem to minimize the performance index, we have

$$F_{\mathrm{ref}} = \begin{bmatrix} -2.17 & -2.67 & -0.79\\ -1.79 & -3.12 & -4.66\end{bmatrix}.$$

Table 2 shows device situations where the control system with this design is stable. The sufficiently small performance index in the normal case implies that the control system has desirable disturbance attenuation performance. However, if at least one device fails, i.e., in the other 31 situations than the normal case, it is unstable. Hence this is the reference case.

There are many cases where we obtain such a fragile control system if we look only for the optimality in a performance index. It is not unrealistic to consider the reference case where the control system falls into an unstable state and a demand on an E/E/PE SRS occurs if only one device fails.

Table 2. Stable device situations in the reference case.

| Situation | Normal case |
|---|---|
| Poles | $-1.95$<br>$-1.44+j0.70$<br>$-1.44-j0.70$ |
| $\|T_{zw}\|_2$ | 6.50 |

In the reference case, the demand rate is

$$\mathrm{DR}_{\mathrm{ref}} = \lambda_{\mathrm{all}} = 1.50\times 10^{-4}[1/\mathrm{hour}]$$

and the mean time to demand is

$$\mathrm{MTTD}_{\mathrm{ref}} = \frac{1}{\lambda_{\mathrm{all}}} = 6.67\times 10^{3}[\mathrm{hour}].$$

Hence, under Assumption 3, the demand frequency in the reference case is

$$\mathrm{DF}_{\mathrm{ref}} \approx \lambda_{\mathrm{all}} = 1.50\times 10^{-4}[1/\mathrm{hour}].$$

### *B. Step 2: target demand frequency*

Suppose that the target hazard frequency is $\mathrm{HF}_{\mathrm{tar}} = 10^{-7}[1/\mathrm{hour}]$.

In the reference case,

$$\mathrm{PFD}_{\mathrm{ref}} \le \frac{10^{-7}[1/\mathrm{hour}]}{1.50\times 10^{-4}[1/\mathrm{hour}]} = 6.67\times 10^{-4}.$$

Hence we should install an E/E/PE SRS of SIL 3 in order to achieve the target hazard frequency (see Table 1(a)).

Here we set

$$\mathrm{DF}_{\mathrm{tar}} = \frac{2}{3}\times 10^{-4}[1/\mathrm{hour}] = 6.67\times 10^{-5}[1/\mathrm{hour}].$$

Then

$$\mathrm{PFD}_{\mathrm{req}} \le \frac{10^{-7}[1/\mathrm{hour}]}{\frac{2}{3}\times 10^{-4}[1/\mathrm{hour}]} = 1.50\times 10^{-3}.$$

Hence it is enough to install an E/E/PE SRS of SIL 2 in order to achieve the target hazard frequency.

Table 3. Stable device situations in the control system with the control logic to be evaluated.

| Situation | Normal case | Device 1 fault | Device 3 fault | Device 4 fault | Device 5 fault |
|---|---|---|---|---|---|
| Poles | $-10.57$<br>$-0.39+j0.12$<br>$-0.39-j0.12$ | $-0.20$<br>$-2.08+j4.39$<br>$-2.08-j4.39$ | $-3.39$<br>$-0.79+j0.98$<br>$-0.79-j0.98$ | $-3.12$<br>$-0.63+j0.19$<br>$-0.63-j0.19$ | $-2.87$<br>$-1.63$<br>$-0.47$ |
| $\|T_{zw}\|_2$ | 32.00 | — | — | — | — |

The safety function in a controller, i.e., a logic solver, designed by reliable control reduces a burden on an E/E/PE SRS. This is a concrete contribution of reliable control to risk reduction in accordance with IEC 61508.

### C. Step 3: target safety measures against device faults

Consider

$$\mathrm{SM} = \{\{1\},\{3\},\{4\},\{5\}\}.$$

Then, using (14), we have

$$\begin{aligned}\mathrm{MTTD}(\mathrm{SM}) &= \left[\frac{1}{a_{\{1\}}} - \frac{a_{\{1\}}}{\lambda_{\mathrm{all}}^2}\right] + \left[\frac{1}{a_{\{3\}}} - \frac{a_{\{3\}}}{\lambda_{\mathrm{all}}^2}\right] \\ &\quad + \left[\frac{1}{a_{\{4\}}} - \frac{a_{\{4\}}}{\lambda_{\mathrm{all}}^2}\right] + \left[\frac{1}{a_{\{5\}}} - \frac{a_{\{5\}}}{\lambda_{\mathrm{all}}^2}\right] + \frac{\lambda_2}{\lambda_{\mathrm{all}}^2} \\ &= 1.54\times 10^4[\mathrm{hour}].\end{aligned}$$

Under Assumption 3, the demand frequency is

$$\mathrm{DF}(\mathrm{SM}) = \frac{1}{\mathrm{MTTD}(\mathrm{SM})} = 6.50\times 10^{-5}[1/\mathrm{hour}] < \mathrm{DF}_{\mathrm{tar}}.$$

Hence we can choose this SM as target safety measures, $\mathrm{SM}_{\mathrm{tar}}$, i.e.,

$$\mathrm{SM}_{\mathrm{tar}} = \{\{1\},\{3\},\{4\},\{5\}\}.$$

### D. Step 4: controller design by reliable control theory

We have the following feedback-gain matrix by a similar design method presented in [4] with the target safety measures obtained in Step 3:

$$F = \begin{bmatrix} -6.97 & -10.17 & -13.56 \\ -3.70 & -5.00 & -6.37 \end{bmatrix}.$$

### E. Step 5: controller evaluation

Next, consider the control system with the control logic to be evaluated. Table 3 shows device situations where the control system with the designed $F$ is stable. Although the disturbance attenuation performance in the normal case is worse as compared with the reference case, the stability of the control system can be maintained even if one of Devices 1, 3, 4 and 5 fails as the target safety measures.

## VI. Conclusion

The presented safety performance index can be used in controller designed by almost all reliable control. No studies have ever tried to set a target safety integrity as one of control performance indices in controller design. We should draw attention not only to the importance of the performance index in IEC 61508 but also to its contribution to the further theoretical advance in reliable control theory.

## References

[1] M. Fujita and E. Shimemura, ”Integrity against arbitrary feedback-loop failure in linear multivariable control,” *Automatica*, Vol.24, No.6, pp.765–772, 1988.

[2] C. Garrett and G. Apostolakis, ”Context in the risk assessment of digital systems,” *Risk Analysis*, Vol.19, pp.23–32, 1999.

[3] A. N. Gündeş, ”Stability of feedback systems with sensor or actuator failures: analysis,” *Int. J. Control*, Vol.56, No.4, pp.735–753, 1992.

[4] Y. Hamada, S. Shin and N. Sebe, ”A design method for fault-tolerant control systems based on $H_\infty$ optimization,” *Proc. 35th IEEE CDC*, pp.1918–1919, 1996.

[5] Health & Safety Executive (HSE), *Out of Control — Why control systems go wrong and how to prevent failure*, HSE Books, 1995.

[6] E. J. Henley and H. Kumamoto, *Probabilistic Risk Assessment: Reliability Engineering, Design, and Analysis*, IEEE Press, 1992.

[7] *IEC 61508: Functional safety of electrical/electronic/ programmable electronic safety related systems*, 1998–2000.

[8] *ISO/IEC Guide 51: Guidelines for the inclusion of safety aspects in standards*, 1990.

[9] *ISO/IEC Guide 51 (E): Guidelines for the inclusion of safety aspects in standards*, 2nd edition, 1999.

[10] K. D. Minto and R. Ravi, ”New results on the multi-controller scheme for the reliable control of linear plants,” *Proc. 1991 ACC*, pp.615–619, 1991.

[11] N. Sebe, ”Diagonal dominance and integrity,” *Proc. 35th IEEE CDC*, pp.1904–1909, 1996.

[12] K. Suyama and G. Apostolakis, ”A new direction of reliable control: a context-based approach,” *Proc. 2000 ACC*, pp.352–358, 2000.

[13] K. Suyama and G. Apostolakis, ”A context-based approach to reliable control: context-dependent performance,” *Proc. 2001 ACC*, pp.1027–1034, 2001.

[14] K. Suyama, ”Advanced cooperative order in a compensator set in passive redundancy,” *IEEE Trans. Automat. Contr.*, Vol.46, No.7, pp.1151–1155, 2001.

[15] K. Suyama, ”Context-based reliable control,” *Proc. ECC*, pp.1273–1278, 2001.

[16] K. Suyama, ”Systematization of reliable control,” *Proc. 2002 ACC*, pp.5110–5118, 2002.

[17] K. Suyama, ”What is reliable control?” *Proc. 15th IFAC World Congress*, 2002.

[18] K. Suyama, ”Safety integrity analysis framework for a controller according to IEC 61508,” *Proc. 42nd IEEE CDC*, pp.2477–2483, 2003.

[19] R. J. Veillette, J. V. Medanić and W. R. Perkins, ”Design of reliable control systems,” *IEEE Trans. Automat. Contr.*, Vol.37, No.3, pp.290–304, 1992.

[20] R. J. Veillette, ”Reliable linear-quadratic state feedback control,” *Automatica*, Vol.31, pp.137–143, 1995.

[21] M. Vidyasagar and N. Viswanadham, ”Reliable stabilization using a multi-controller configuration,” *Automatica*, Vol.21, No.5, pp.599–602, 1985.

[22] G. H. Yang, J. Lam and J. Wang, ”Reliable $H_\infty$ control for affine nonlinear systems,” *IEEE Trans. Automat. Contr.*, Vol.43, No.8, pp.1112–1117, 1998.

[23] G. H. Yang, J. Wang and Y. C. Soh, ”Reliable $H_\infty$ control for linear systems with sensor failures,” *Proc. 37th IEEE CDC*, pp.2822–2827, 1998.

[24] G. H. Yang, J. L. Wang and Y. C. Soh, ”Reliable LQG control with sensor failure,” *Proc. 38th IEEE CDC*, pp.3564–3568, 1999.

[25] J. S. Yee, J. L. Wang and G. H. Yang, ”Reliable output feedback controller design for discrete-time linear systems: an approach,” *Proc. 2001 ACC*, pp.1035–1040, 2001.