PROBABILISTIC SAFETY ASSESSMENT OF CONTROL LAWS BASED ON IEC STANDARDS

Koichi Suyama *

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

Abstract: This paper presents a probabilistic safety assessment framework based on the international standard, IEC 61508, for control laws designed especially by reliable control theory. The framework uses Markov techniques summarized in IEC 61165 to take restoration of devices into consideration. It clarifies a contribution of reliable control to risk reduction required in IEC 61508. *Copyright ©2005 IFAC*

Keywords: Safety, standards, control laws, Markov models, fault-tolerant systems.

1. INTRODUCTION

The social environment surrounding system safety has changed rapidly. One of the epochs was that TC65 WGs 9 and 10 in IEC, International Electrotechnical Commission, established an international standard, IEC 61508 (1998–2000). It is applied to almost all electrical/electronic/ programmable electronic (E/E/PE) safety-related systems (SRSs) irrespective of their applications.

Since the late 1970s many studies have been made on control system design under possible device failures, such as integrity (Fujita and Simemura, 1988), reliable $\mathcal{H}_\infty$ control (Veillette *et al.*, 1992).

Recently the importance of safety function realized in a control system has been growing. One of the reasons is that ISO/IEC Guide 51 (1999) adopted newly risk to the environment and to property as its scope. It is widely known that there are many cases where safety measures outside a control system are not enough to reduce risk to property or to the environment. 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 (Suyama, 2002).

This paper presents a probabilistic safety assessment framework based on IEC 61508 for control laws designed especially by reliable control theory. The presented framework uses Markov techniques summarized in IEC 61165 (1995) [1] to take restoration of control devices into consideration. It is more practical than the one in Suyama (2003), which pays attention only to o device failures.

The presented framework clarifies a concrete contribution of reliable control to risk reduction required in IEC 61508, i.e., an important role of reliable control in system safety design.

IEC 61508 is now under maintenance [2]. A safety assessment framework for software used in safety-related systems will newly be prepared for publication. If we design safety function in a control law, we should assess its safety integrity quantitatively.The presented framework, which is ahead of the times, will be reflected to IEC 61508.

[1] The author is a member of IEC TC56 WG2, which takes charge of IEC 61165. The presented safety assessment framework is one of important applications of Markov techniques in the field of control engineering.

[2] The author is a member of the maintenance team MT-13 for IEC 61508.

2. IEC 61508 AND RELIABLE CONTROL

Figure 1 illustrates the overall system configuration considered in IEC 61508. The original control system consists of an equipment under control (EUC), i.e., a controlled object, and a basic control system (BCS) 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, i.e., EUC+BCS risk, by E/E/PE SRSs and/or other technology SRSs and external risk reduction facilities (ERRFs) so that the residual risk of the overall system is less than the predetermined tolerable risk level as shown in Figure 2.

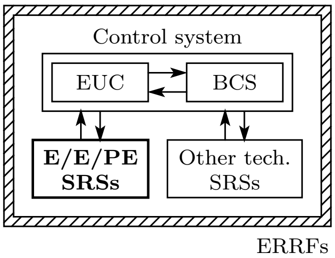

Figure 1. Overall system.

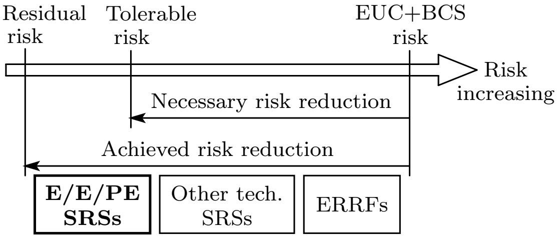

Figure 2. Risk reduction.

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

SIL	Average probability of failure to perform its design function on demand (PFD_{avg})
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 $< 10^{-1}$

A SRS 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 assesses 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, low demand mode of operation as shown in Table 1 and high demand / continuous mode. If a SRS shoulders a heavy burden for risk reduction, it is required to fit a higher SIL.

Reliable control realizes safety function against device failures in the redundancy in the sense of productivity or efficiency at the sacrifice of control performance in the normal operation (Suyama, 2002). Because it is sufficient that risk reduction in Figure 2 is achieved as the overall system, the safety function achieved by reliable control can be complementary to SRSs as shown in Figure 3.

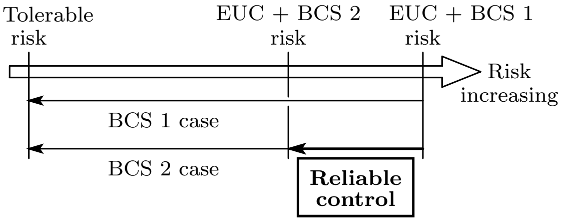

Figure 3. Necessary risk reduction.

Due to the functional safety realized by reliable control in BCS 2, the risk of the control system EUC + BCS 2 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.

It is contribution of reliable control to risk reduction in IEC 61508. The probabilistic safety assessment framework for control laws presented in the following section clarifies the contribution quantitatively.

3. PROBABILISTIC SAFETY ASSESSMENT FRAMEWORK FOR CONTROL LAWS

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 λ_i, $i = 1, \ldots, N$. Restoration of failed Device i probabilistically completes in accordance with the exponential distribution with the repair rate μ_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 low demand mode of operation in IEC 61508 and makes the meaning of the presented safety assessment framework clear.

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

- stability degree, or
- permissible deterioration in control performance.

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).

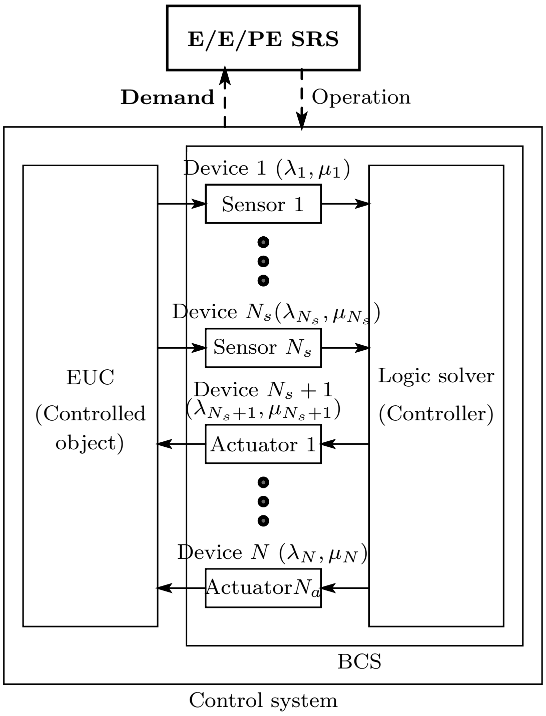

Figure 4. Control system and SRS.

The presented safety assessment framework for control laws is based on 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.

The presented safety analysis framework consists of the following steps:

Step 0: analysis of reference case for comparison with the assessed control law
Step 1: (for the assessed control law, and so forth) obtaining a set of all stable device situations
Step 2: description of demand occurrence in a Markov model, i.e., a state transition diagram,
Step 3: calculation of demand frequency, and
Step 4: SIL assignment to a SRS.

3.1 Step 0: 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 control law without any safety functions is used.

Define

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

Then, the demand rate in the reference case is

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

and the mean time to demand is

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

In general, a demand frequency is given by

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

where MTTR denotes a mean time to repair of the overall system.

Assumption 3:

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

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

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

This is the safety integrity of a control law without any safety functions, which should be compared with the assessed control law.

3.2 Step 1: stable device situations

Each device is in either of normal: 0 or fault: 1. Hence, as a whole, the control system with N devices is in one of 2^N device situations. By stability analysis of all possible situations one by one, we can obtain all stable device situations, SS, except the normal operation, e.g.,

$$\begin{aligned} \text{SS} = \{ \;& (1,0,0,0,\ldots,0) : \\ & \quad \text{only Device 1 is in a fault,} \\ & (0,1,1,0,\ldots,0) : \\ & \quad \text{only Devices 2 and 3 are in faults,} \\ & (0,0,1,0,\ldots,0) : \\ & \quad \text{only Device 3 is in a fault,} \\ & (1,0,1,0,\ldots,0) : \\ & \quad \text{only Devices 1 and 3 are in faults,} \\ & \quad \cdots \}. \end{aligned}$$

If the control system is in either the normal operation or one situation of SS, it maintains its stability. However if it transfers to another situation, it falls into an unstable state and a demand on an E/E/PE SRS occurs.

3.3 Step 2: Markov model

Consider device groups, $\mathrm{G}_{(i)} = \big\{\text{Device } i_1, \ldots, \text{Device } i_{n_i}\big\}$ $(i = 1, \ldots, M)$, such that

$$\mathrm{G}_{(i)} \cap \mathrm{G}_{(j)} = \phi, \quad i \neq j. \tag{7}$$

Let $\mathrm{S}_{(i)}$ denote the sets of $2^{n_i} - 1$ device situations only with all possible normal/fault combinations of devices in $\mathrm{G}_{(i)}$. For example, $\mathrm{G}_{(i)} = \big\{\text{Device 1, Device 2}\big\}$, then $\mathrm{S}_{(i)} = \big\{(1,0,0,\ldots), (0,1,0,\ldots), (1,1,0,\ldots)\big\}$. Suppose that

$$\mathrm{SS} = \bigcup_{i=1}^{M} \mathrm{S}_{(i)}. \tag{8}$$

If there does not exist such a set of groups, we choose $\mathrm{G}_{(i)}$ $(i = 1, \ldots, M)$ by maximizing MTTD presented in the following section subject to the constraint that $\mathrm{SS} \supset \bigcup_{i=1}^{M} \mathrm{S}_{(i)}$. Define a group of the rest devices as $\mathrm{G}_{(0)} = \{\text{Device } 1, \ldots, \text{Device } N\} \setminus \bigcup_{i=1}^{M} \mathrm{G}_{(i)}$.

For $\mathrm{G}_{(i)}$ $(i = 1, \ldots, M)$ and $\mathrm{G}_{(0)}$, define

$$\lambda_{(i)} = \sum_{j=1}^{n_i} \lambda_{i_j}, \quad \lambda'_{(i)} = \lambda_{\mathrm{all}} - \lambda_{(i)} \tag{9}$$

$$\lambda_{(0)} = \lambda_{\mathrm{all}} - \sum_{i=1}^{M} \lambda_{(i)}. \tag{10}$$

Assumption 4: Simultaneous restoration of each group $\mathrm{G}_{(i)}$, $i = 1, \ldots, M$, probabilistically completes in accordance with the exponential distribution with the repair rate

$$\mu_{(i)} = \min_{j=1,\ldots,n_i} \mu_{i_j} \tag{11}$$

regardless of the number of failed devices.

Note that simultaneous restoration with the smallest repair rate in a device group gives a conservative assessment result.

Figure 5 describes the state transition from the normal operation $\mathrm{S}_{(0)}$ to demand occurrence, i.e., unstable state of the control system, $\mathrm{S}_{(M+1)}$. The arrows with $\lambda_{(1)}$ and with $\mu_{(1)}$ denote a failure and restoration in $\mathrm{G}_{(1)}$, respectively. The arrow with $\lambda'_{(1)}$ denotes a failure in another device than $\mathrm{G}_{(0)}$ on the state $\mathrm{S}_{(1)}$. The arrow with $\lambda_{(0)}$ denotes a failure in $\mathrm{G}_{(0)}$.

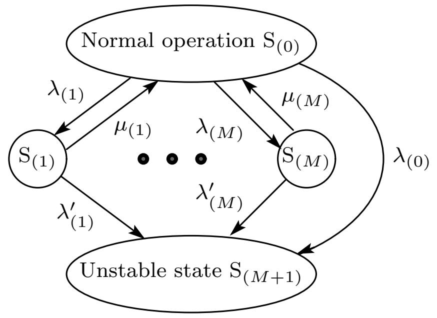

Figure 4. State transition diagram.

3.4 Step 3: demand frequency

Let $p_{(0)}(t)$, $p_{(i)}(t)(i = 1, \ldots, M)$, $p_{(M+1)}(t)$ be the probabilities of the control system being in $\mathrm{S}_{(0)}$, $\mathrm{S}_{(i)}$, $\mathrm{S}_{(M+1)}$ respectively at time t. The following differential equation is obtained from the state transition diagram shown in Figure 4:

$$\frac{d}{dt} p(t) = A p(t) \tag{12}$$

where

$$p(t) = \begin{bmatrix} p_{(0)}(t) \\ p_{(1)}(t) \\ \vdots \\ p_{(M)}(t) \\ p_{(M+1)}(t) \end{bmatrix}$$

$$A = \begin{bmatrix} -\lambda_{\mathrm{all}} & \mu_{(1)} & \cdots & \mu_{(M)} & 0 \\ \lambda_{(1)} & -(\mu_{(1)} + \lambda'_{(1)}) & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \lambda_{(M)} & 0 & \cdots & -(\mu_{(M)} + \lambda'_{(M)}) & 0 \\ \lambda_{(0)} & \lambda'_{(1)} & \cdots & \lambda'_{(M)} & 0 \end{bmatrix}.$$

At time $t = 0$, the control system is in $\mathrm{S}_{(0)}$, i.e.,

$$p(0) = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix}. \tag{13}$$

Define

$$R_S(t) = p_{(0)}(t) + p_{(1)}(t) + \cdots + p_{(M)}(t). \tag{14}$$

Then, using the Markov technique summarized in IEC 61165 (1995), we can obtain the mean time to demand, i.e., the mean time to the first transition to $\mathrm{S}_{(M+1)}$, as follows:

$$\mathrm{MTTD} = \int_0^\infty R_S(t)dt = q_0 + \sum_{i=1}^{M} q_i \tag{15}$$

where

$$q_0 = \left[\lambda_{\mathrm{all}} - \sum_{i=1}^{M} \frac{\lambda_{(i)}\mu_{(i)}}{\mu_{(i)} + \lambda'_{(i)}}\right]^{-1}$$

$$q_i = \frac{\lambda_{(i)}}{\mu_{(i)} + \lambda'_{(i)}} q_0, \quad i = 1, \ldots, M.$$

Then the demand rate is given by

$$\mathrm{DR} = \frac{1}{\mathrm{MTTD}}. \tag{16}$$

Hence, under Assumption 3, we can obtain the demand frequency as follows:

$$\mathrm{DF} \approx \mathrm{DR} = \frac{1}{\mathrm{MTTD}}. \tag{17}$$

3.5 Step 4: SIL assignment to SRS

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

$$\mathrm{HF} = \mathrm{DF} \times \mathrm{PFD}_{\mathrm{avg}}. \tag{18}$$

Hence, given a target hazard frequency, $\mathrm{HF}_{\mathrm{tar}}$, we can obtain a required $\mathrm{PFD}_{\mathrm{avg}}$ by

$$\mathrm{PFD}_{\mathrm{avg}} = \frac{\mathrm{HF}_{\mathrm{tar}}}{\mathrm{DF}} \tag{19}$$

and a required SIL by Table 1. We should install an E/E/PE SRS with the required SIL.

The lower demand frequency, the better control law in the sense of system safety. An 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.

4. EXAMPLE

A control system consists 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 law in a logic solver. Suppose that

$$\begin{aligned}
&\lambda_1 = 2.00 \times 10^{-5}[1/\mathrm{h}],\ \mu_1 = 1.00 \times 10^{-1}[1/\mathrm{h}]\\
&\lambda_2 = 1.00 \times 10^{-5}[1/\mathrm{h}]\\
&\lambda_3 = 5.00 \times 10^{-5}[1/\mathrm{h}],\ \mu_3 = 2.00 \times 10^{-1}[1/\mathrm{h}]\\
&\lambda_4 = 2.00 \times 10^{-5}[1/\mathrm{h}],\ \mu_4 = 1.00 \times 10^{-1}[1/\mathrm{h}]\\
&\lambda_5 = 5.00 \times 10^{-5}[1/\mathrm{h}],\ \mu_5 = 2.00 \times 10^{-1}[1/\mathrm{h}]
\end{aligned}$$

where the value of μ_2 is not used in this example. The plant consisting of the controlled object, the three sensors, and the two actuators is given by

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

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

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 $\mathcal{H}_2$-norm. We design state feedback

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

where the gain matrix

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

is the essence of the assessed control law.

4.1 Step 0: analysis of reference case

Solving a full-information two-block $\mathcal{H}_2$ 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 stable device situations of the control system with this design. The sufficiently small performance index in the normal operation 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 operation, 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.

Table 2. Stable device situations in the reference case.

Situation	Normal operation
Poles	-1.95 $-1.44 + j0.70$ $-1.44 - j0.70$
$\|T_{zw}\|_2$	6.50

In the reference case,

$$\begin{aligned}
\mathrm{DR}_{\mathrm{ref}} &= \lambda_{\mathrm{all}} = 1.50 \times 10^{-4}[1/\mathrm{h}] \\
\mathrm{MTTD}_{\mathrm{ref}} &= \frac{1}{\lambda_{\mathrm{all}}} = 6.67 \times 10^{3}[\mathrm{h}].
\end{aligned}$$

Under Assumption 3, the demand frequency is

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

4.2 Step 1: stable device situations

Next, consider the control system with the assessed control law. Table 3 shows all stable device situations. Then

Table 3. Stable device situations of the system with the assessed control law.

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

Table 4. Markov model of the system with the assessed control law.

Group	Devices	$\lambda_{(i)}$[1/h]	$\mu_{(i)}$[1/h]	$\lambda'_{(i)}$[1/h]
$\mathrm{G}_{(1)}$	Device 1	$\lambda_1 = 2.00 \times 10^{-5}$	$\mu_1 = 1.00 \times 10^{-1}$	$\lambda_2 + \lambda_3 + \lambda_4 + \lambda_5 = 1.30 \times 10^{-4}$
$\mathrm{G}_{(2)}$	Device 3	$\lambda_3 = 5.00 \times 10^{-5}$	$\mu_3 = 2.00 \times 10^{-1}$	$\lambda_1 + \lambda_2 + \lambda_4 + \lambda_5 = 1.00 \times 10^{-4}$
$\mathrm{G}_{(3)}$	Device 4	$\lambda_4 = 2.00 \times 10^{-5}$	$\mu_4 = 1.00 \times 10^{-1}$	$\lambda_1 + \lambda_2 + \lambda_3 + \lambda_5 = 1.30 \times 10^{-4}$
$\mathrm{G}_{(4)}$	Device 5	$\lambda_5 = 5.00 \times 10^{-5}$	$\mu_5 = 2.00 \times 10^{-1}$	$\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 = 1.00 \times 10^{-4}$
$\mathrm{G}_{(0)}$	Device 2	$\lambda_2 = 1.00 \times 10^{-5}$	—	—

$$\mathrm{SS} = \{\ (1,0,0,0,0),\ (0,0,1,0,0),\\ (0,0,0,1,0),\ (0,0,0,0,1)\ \}.$$

Although the disturbance attenuation performance in the normal operation 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.

4.3 Step 2: Markov model

See Table 4.

4.4 Step 3: demand frequency

From (15),

$$\mathrm{MTTD} = 3.91 \times 10^4[\mathrm{h}].$$

Here the mean time to demand is over twice as long as the reference case. Under Assumption 3, the demand frequency is

$$\mathrm{DF} \approx \mathrm{DR} = \frac{1}{\mathrm{MTTD}} = 1.01 \times 10^{-5}[1/\mathrm{h}].$$

The demand frequency reduction rate against the reference case is

$$\frac{\mathrm{DF}}{\mathrm{DF}_{\mathrm{ref}}} = \frac{1.01 \times 10^{-5}[1/\mathrm{h}]}{1.50 \times 10^{-4}[1/\mathrm{h}]} = 0.0673.$$

This indicates the safety integrity performance of the assessed control law.

4.5 Step 4: SIL assignment to SRS

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

In the reference case,

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

We should install an E/E/PE SRS of SIL 3 achieve the target hazard frequency (see Table 1).

On the other hand, in the control system with the assessed control law,

$$\mathrm{PFD}_{\mathrm{avg}} = \frac{10^{-7}[1/\mathrm{h}]}{1.01 \times 10^{-5}[1/\mathrm{h}]} = 9.90 \times 10^{-3}.$$

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

5. CONCLUSION

The presented safety assessment framework can be applied to control laws designed by almost all reliable control. No studies have ever tried to analyze safety integrity of control laws probabilistically. We should draw attention not only to the importance of the presented framework in IEC 61508 but also to its contribution to further theoretical advance in reliable control.

REFERENCES

Fujita, M. and E. Shimemura (1988). Integrity Against Arbitrary Feedback-loop Failure in Linear Multivariable Control. *Automatica*, **24**, 765–772.

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

IEC 61165: Application of Markov techniques (1995).

IEC 61508: Functional safety of electrical/electronic/ programmable electronic safety related systems (1998–2000).

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

Suyama, K. (2002). What is reliable control? *Proc. 15th IFAC World Congress.*

Suyama, K. (2003). Safety integrity analysis framework for a controller according to IEC 61508. *Proc. 42nd IEEE CDC*, 2477–2483.

Suyama, K. (2004). Controller design using safety performance index according to IEC 61508. *Proc. 2004 ACC*, 1811–1816.

Veillette, R.J., J.V. Medanić and W.R. Perkins (1992). Design of Reliable Control Systems. *IEEE Trans. Automat. Contr.*, **37**, 290–304.